REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(05-04-07)*

2. REPORT TYPE Masters Thesis

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
The Department of Defense Net-Centric Data Strategy: Implementation Requires a Joint Community of Interest (COI) Working Group and a Joint COI Oversight Council

5a. CONTRACT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Clinton R. Bigger, LTC, USA

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Forces Staff College
Joint Advanced Warfighting School
7800 Hampton, Blvd.
Norfolk, VA 23511-1702

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public released, distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT In 2003, the ASD(NII) DoD CIO published the DoD Net-Centric Data Strategy providing guidance to DoD Components for the development of policies and practices to improve data sharing throughout the DoD. The objective of this strategy is to make data more visible, accessible, and understandable to users of the Global Information Grid (GIG). The stated goal of the strategy is to empower users through faster access to data by posting data prior to processing. The DoD Net-Centric Data Strategy provides a middle management approach to data management through Communities of Interest (COI), the reuse of discovery and content metadata, and use of GIG Enterprise Services (GES). COIs will be responsible for the development of data sharing capabilities in developing Information Technology programs. COIs are encouraged to reuse metadata previously registered by other COIs. Commonly referred to as "data tagging," metadata is the technical link between data stored in the GIG and users searching for data. GES provides the enterprise services for the development of metadata and for data searches. The results of a 2006, Progress and Compliance Report, completed by the ASD(NII) DoD CIO document progress on the part of Mission Areas and DoD Components in creating COIs and establishing data sharing policies. However, in four key findings, the report documented areas that require attention by the DoD to achieve the goals of the DoD Net-Centric Data Strategy. Analysis of the report demonstrates a decentralized approach to developing data sharing policy has emerged and additional guidance is required to ensure DoD Net-Centric Data Strategy goals are met. To effectively implement the strategy, a Joint COI Working Group and Joint COI Oversight Council should be established to provide unity of effort to the creation of DoD data sharing policy and the development of discovery and content metadata standards.

15. SUBJECT TERMS
DoD Net-Centric Data Strategy, Communities of Interest, Metadata, Defense Acquisition

16. SECURITY CLASSIFICATION OF:
Unclassified

a. REPORT Unclassified

b. ABSTRACT Unclassified

c. THIS PAGE Unclassified

17. LIMITATION OF ABSTRACT
Unclassified
Unlimited

18. NUMBER OF PAGES

19a. NAME OF RESPONSIBLE PERSON
SPC Rassmussen

19b. TELEPHONE NUMBER *(include area code)*
757-463-6301

JOINT FORCES STAFF COLLEGE
JOINT ADVANCED WARFIGHTING SCHOOL

THE DEPARTMENT OF DEFENSE NET-CENTRIC DATA STRATEGY: IMPLEMENTATION REQUIRES A JOINT COMMUNITY OF INTEREST (COI) WORKING GROUP AND JOINT COI OVERSIGHT COUNCIL

by

Clinton R. Bigger

Lieutenant Colonel, United States Army

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

Signature:______________________________

17 May 2007

Thesis Adviser: Michael Santacroce, COL, United States Marine Corps

ABSTRACT

In 2003, the Assistant Secretary of Defense for Networks Information and Integration ASD(NII) Department of Defense Chief Information Officer (DoD CIO) published the *DoD Net-Centric Data Strategy*, providing guidance for the development of policies and practices to improve data sharing in the DoD. The objective of the strategy is to make data more visible, accessible, and understandable to users of the Global Information Grid (GIG). The goal is to empower users through faster access to data by posting data prior to processing. The strategy provides a middle management approach to data management through Communities of Interest (COI), reuse of discovery and content metadata, and use of GIG Enterprise Services (GES). COIs are responsible for the development of data sharing capabilities in Information Technology programs. Commonly referred to as "data tagging," metadata is the technical link between data stored in the GIG and users searching for data. GES provides the enterprise services for the development of metadata and for data searches. The 2006, *Net-Centric Data Strategy Progress and Compliance Report,* completed by the ASD(NII) DoD CIO, documents progress on the part of DoD components toward the creation of COIs and establishment of data sharing policies. However, the report also documents areas requiring attention to achieve *DoD Net-Centric Data Strategy* goals. Analysis of the report demonstrates a decentralized approach to developing data sharing policy has emerged and additional guidance is required to ensure *DoD Net-Centric Data Strategy* goals are met. To effectively implement the strategy a Joint COI Working Group and Joint COI Oversight Council should be established to provide unity of effort to the creation of DoD data sharing policy and the development of discovery and content metadata standards.

About the Author

Lieutenant Colonel Clinton R. Bigger received his commission from the University of Northern Iowa in 1986 where he earned a B.A. in Secondary Education with an emphasis in history. He attended the Signal Corps Officer Basic Course at Fort Gordon, GA; the Marine Corps Advanced Communications Course at Quantico, VA; and Command and General Staff College at Fort Leavenworth, KS. From February 2001 to February 2002, he served in OPERATION SOUTHERN WATCH as the Command and Control Systems Chief, J6, Joint Task Force-Southwest Asia (JTF-SWA). He served as the Commander, 304th Signal Battalion, 1st Signal Brigade and as the Deputy Commander, 1st Signal Brigade in the Republic of Korea. In July 2007, he is scheduled for assignment to Multi National Forces-Iraq (MNF-I) as the Deputy Director for Communications and Information Services.

CONTENTS

Appendix

CONTENTS

ILLUSTRATIONS

CHAPTER 1: INTRODUCTION

Advancement in information technology has had a significant impact on how the Department of Defense (DoD) uses communications systems to share information and conduct operations. As joint forces transform and develop increasing degrees of interdependence, the ability to effectively share information grows in importance. The DoD has identified network-centric capabilities as key to improving joint military operations. An integral part of achieving net-centric capabilities is an effective DoD- wide data sharing strategy. The 2006 *National Security Strategy (NSS)*, 2005 *National Defense Strategy (NDS)*, 2006 *Quadrennial Defense Review Report (QDR)*, and the 2004 National *Military Strategy (NMS)* collectively articulate the concept that network-centric capabilities are a desired attribute for joint forces. Specifically, the *QDR* calls for a strengthened data strategy.

In response to the need for an effective DoD-wide data strategy, the Assistant Secretary of Defense for Networks Information and Integration (ASD/NII) and DoD Chief Information Office (CIO) published the 2003 *Department of Defense Net-Centric Data Strategy*. The thesis of this paper is to effectively implement this strategy, a Joint Community of Interest (COI) Working Group and Joint COI Oversight Council should be established to provide unity of effort to the creation of DoD data sharing policy and the development of discovery and content metadata standards which are linked to the Defense Acquisition System (DAS).

The desire of militaries to employ advanced information technology is not a new phenomenon. The British used radar, a new technology in 1939, to identify German aircraft during WWII.[1] By 1966, an early version of data link technology led to the development of improved data links that passed information to and from the Lockheed U2 manned surveillance aircraft during the Vietnam

[1] Martin Van Creveld, *Technology and War from 2000B.C. to Present* (New York: The Free Press, 1991), 192.

War.[2] By the 1991 Gulf War, the United States utilized the Airborne Warning and Control System (AWACS) and Joint Surveillance Target Attack Radar System (JSTARS), two aerial reconnaissance systems, to provide detailed air and ground pictures respectively.[3] Today, use of advanced information technology has resulted in the development of numerous service specific and joint networked communication systems. These systems enable joint U.S. forces to execute operations by linking sensors, weapons, operators, and decision makers using a myriad of communications means. These networked communications systems are connected to the Global Information Grid (GIG), the DoD's global communications architecture, which possesses tremendous information sharing capability. Many of the current network-centric capabilities have made significant contributions to operations in the war on terrorism.[4] One example is the sharing of surveillance video from the Predator Unmanned Aerial Vehicles (UAV) of Afghanistan and Iraq transmitted over satellite radio to command centers in Saudi Arabia, Qatar, and Central Command Headquarters in Tampa Bay, Florida.[5]

Despite improvements in the interoperability of communications systems and the development of network-centric capabilities, operations in Afghanistan and Iraq have demonstrated that data sharing problems still exist. A recent U.S. Government Accounting Office (GAO) report documents comments from Joint Forces Command (JFCOM) and Special Operations Command (SOCOM) that ground forces in Operation Iraqi Freedom possess Blue Force Tracking systems, used to track

[2] Barry Press, "Net Effect: Barry Press, chief engineer at L-3 Communications, Communications Systems West, describes how networked data links enhance situational awareness," *C4ISR: The Journal of Net-Centric Warfare* (Springfield) Vol. 5, No. 4 (May 2005), 42.

[3] Williamson Murray and Robert H. Scales Jr., *The Iraq War: A Military History* (Cambridge: Belknap Press of Harvard Press, 2003), 268-270.

[4] U.S. Department of Defense, *The National Defense Strategy of the United States of America* (Washington, D.C.: Government Printing Office, 2005), 14.

[5] United States General Accounting Office, *GAO Report to Congressional Committees; Military Operations; Recent Campaigns Benefited from Improved Communications and Technology, but Barriers to Continued Progress Remain* (Washington, D.C.: GAO 2004), 14-15.

friendly ground forces, which did not share data.[6] Resolution of information sharing issues is paramount to effective joint operations, which is why network-centric capabilities, including data sharing, received attention as a priorities in the *NSS*, *NDS*, *QDR*, and *NMS*.

The ASD/NII) and DoD CIO recognized the need for a strengthened data strategy and published the 2003 *Department of Defense Net-Centric Data Strategy*. Guidance supporting the *DoD Net-Centric Data Strategy* is contained in the 2004 *DoD Directive 8320.2, Data Sharing in a Net-Centric Department of Defense* and 2006 *DoD 8320-G, Guidance for Implementing Net-Centric Data Sharing*. The goals of the *DoD Net-Centric Data Strategy* stated by the DoD Chief Information Office (CIO) are as follows:

> Ensuring data are visible, available, and usable when needed and where needed to accelerate decision making.
>
> "Tagging" of all data (intelligence, non-intelligence, raw, and processed) with metadata to enable discovery of data by users.
>
> Posting of all data to shared spaces to provide access to all users except when limited by security, policy or regulations.
>
> Advancing the Department from defining interoperability through point-to-point interfaces to enabling the "many-to-many" exchanges typical of a net-centric data environment.[7]

The purpose of the *DoD Net-Centric Data Strategy* is to strengthen data sharing throughout the DoD. This is accomplished by transitioning to a "many-to-many" data exchange environment to enable many users to leverage the same data as opposed to the current data exchange environment focused on standardized, defined, point-to-point interfaces.[8] The objective of the *DoD Net-Centric Data Strategy* is to improve information sharing by making data more visible, available, and usable,

[6] Ibid., 19-23.

[7] U.S. Department of Defense, *Chief of Information Office Memorandum, Subject: DoD Net-Centric Data Strategy* (Washington, D.C.: Government Printing Office, 2003), 1-2.

[8] U.S. Department of Defense, *Department of Defense Net-Centric Data Strategy* (Washington, D.C.: Government Printing Office, 2003), ii.

when and where needed, to accelerate decision cycles.[9] The goal of the strategy is to empower users through faster access of data by posting data to shared space prior to processing.[10] Accomplishing the objective and goals of the *DoD Net-Centric Data Strategy,* by providing a "many-to-many" and "post and smart-pull" information environment, will enable decision superiority by making relevant data more readily available.

In the past, data sharing was a product of top down management through the publication of technical standards for operating on the GIG. Program developers adhered to technical standards, but no process ensured procedures were in place to meet data sharing goals as now defined in the *DoD Net-Centric Data Strategy*. Data sharing attributes, built into a system, are based on system specific interfaces to support a specific set of users. These systems merely had to meet technical standards established by the Defense Information Systems Agency (DISA). The *DoD Net-Centric Data Strategy* provides a middle management approach to data management through Communities of Interest (COI), use of common discovery and content meta-data schemes, and GIG Enterprise Services.[11] COIs will serve as the primary organizations responsible for the development of data sharing attributes in a system or program.

A significant task accomplished by COIs is the development and registry of discovery and content metadata. Discovery and content metadata, commonly referred to as "data tagging," are data schemes used to identify data assets stored in shared spaces throughout the GIG. Discovery and content metadata include taxonomy and ontology, which form the structure, vocabulary, and thesaurus information, to describe a data asset. Discovery and content metadata is associated with the data asset in shared space, making it accessible to users through search engines. Discovery and

[9] Ibid., ii.
[10] Ibid., ii.
[11] Ibid., 4.

content metadata is the technical link between the user searching for a data asset and the data asset stored in shared space. The *DoD Net-Centric Data Strategy* defines a data asset as follows:

> Data asset refers to any entity that is composed of data. For example, a database is a data asset that comprises data records. In this document, "data asset" means system or application output files, databases, documents or web pages. Data asset also includes services that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a website that returns data in response to specific queries (e.g. weather.com) would be a data asset.[12]

COIs register system discovery and content meta-data schemes with the Defense Information Systems Agency Registry (DISR). *DoD 8320.02-G* states that COIs should identify opportunities to reuse previously registered discovery and content meta-data.[13] GIG Enterprise Services, managed by DISA through Net-Centric Enterprise Services (NCES), provide the metadata formats, metadata repositories, enterprise portals and federated search engines that make data visible, available, and usable to users throughout the GIG. COIs are linked to the Joint Capabilities Integration and Development System (JCIDS) and Defense Acquisition System (DAS) through interaction between the COI and Joint Portfolio Management Mission Areas.

The *DoD Net-Centric Data Strategy* is supported by JCIDS and DAS through the requirements for an Information Support Plan (ISP) with integrated architectures, Net-Ready Key Performance Parameters (NR-KPP), and registration of discovery and content with DISA. ISPs and NR-KPPs are intended to enforce data exchange requirements as programs progress through the JCIDS and DAS process. The ISP, which documents the information sharing needs of a program, is a required component in key JCIDS documents as a program progresses through the DAS. NR-KPPs and their associated GIG Key Interface Profiles (GIG-KIP) provide specific requirements for data exchange in a program to achieve milestone decision approval in the DAS.

[12] Ibid., A-1.

[13] U.S. Department of Defense, *DoD 8320.02-G, Guidance for Implementing Net-Centric Data Sharing* (Washington, D.C.: Government Printing Office, 2006), 19.

Implemented as written, the aforementioned guidance will achieve a degree of data sharing improvement. However, implementation of the guidance is leading to a decentralized approach to the development of mission area and DoD component COI governance processes that do not provide adequate unity of effort into this DoD wide program. Additionally, the guidance does not adequately enforce the use of common discovery and content metadata. COIs are only encouraged to reuse discovery and content metadata previously registered by other COIs. Additionally, COIs are not required to use standard taxonomy and ontology.

The challenge in strengthening DoD data sharing is compounded by the size and complexity of the Global Information Grid (GIG). The GIG has grown dramatically in the number of users, systems, software applications, and communications systems that collect, share, and transport data. The size and complexity of the GIG does not lend itself to a decentralized data management approach if data sharing goals are to be met.

To effectively implement the *DoD Net-Centric Data Strategy* the DoD should establish a Joint COI Working Group, responsible for the development of *DoD Net-Centric Data Strategy* policy, and a Joint COI Oversight Council, responsible for the approval of future *DoD Net-Centric Data Strategy* policy and oversight of mission area and DoD component COI activities. Additionally, the Joint COI Working Group and Joint COI Oversight Council should be responsible for the development of discovery and content metadata standards for mission areas and DoD component like functional areas not managed by a mission area. These discovery and content metadata standards should then be integrated into JCIDS and DAS.

The strategy of this paper is to first, describe the national strategic guidance that defines and directs the development of joint forces net-centric capabilities in order to provide a framework for understanding the necessity of implementing the *DoD Net-Centric Data Strategy*. Second, the study will define and describe net-centricity and the goal to achieve a "many-to-many" and "post and smart-pull" data exchange information environment. Third, the paper will describe the *DoD Net-Centric Data Strategy* as an essential DoD-wide effort to develop net-centric capabilities. Fourth, this study will highlight the *DoD Net-Centric Data Strategy and Progress and Compliance Report* that describes progress and identifies issues in strategy implementation. Finally, the paper will provide recommendations with supporting analysis to establish a Joint COI Working Group and Joint COI Oversight Council. The recommended Joint COI Working Group and Joint COI Oversight Council will provide unity of effort to *DoD Net-Centric Data Strategy* policy across the DoD including the development standards for discovery and content metadata.

CHAPTER 2: NETWORK-CENTRICITY

Network-centric capability is the concept of a force that is best equipped and trained to execute operations maximizing the operational benefits gained through the use of interoperable communications systems linking sensors, weapons, operators, and decision makers. This capability facilitates accurate awareness of the enemy and friendly battlefield situation, provides timely actionable information to decision makers, and reduces the time between sensing and destroying a target. This is accomplished through quick and accurate sharing of relevant information. The *NDS* defines network-centric capability as follows:

> Network-centric operational capability is achieved by linking compatible information systems with usable data. The functions of sensing, decision-making, and acting--which often in the past were built into a single platform--can now work closely even if they are geographically distributed across the battlespace.[14]

The need to develop Net-Centric capable forces is a theme that runs through current national and DoD strategic security guidance. Developing net-centric capable forces is dependent upon the appropriate use of computer networking technology to achieve a "many-to-many" and "post and smart-pull" information environment. Developing Net-Centric capabilities also is dependent upon a GIG that has grow to such size and complexity that it requires centralized governance for DoD wide GIG data sharing.

National Strategic Guidance

[14] U.S. Department of Defense, *The National Defense Strategy of the United States of America,* 14.

The *NSS*, *NDS*, *QDR*, and *NMS* provide the DoD with strategic planning guidance for development of operational plans and defense transformation. These documents identify network-centric capabilities as a key joint forces operational capability and as an initial joint capability portfolio test case for acquisition management. The purpose of using joint capability portfolios is to improve management of major acquisition programs by governing these programs in capability groups rather than individual programs. A Deputy Secretary of Defense memorandum describes the intent of capability portfolio management as, "to manage groups of like capabilities across the enterprise to improve interoperability, minimize capability redundancies and gaps, and maximize capability effectiveness."[15] Network-centric operations received priority when it was identified in the *QDR* as one of the first of eight capability areas to be managed by capability portfolio.[16]

The *NSS,* as the foundation for the United States Government strategic planning, makes no direct reference to network-centric capabilities. However, the *NSS* does provide implied guidance to develop network-centric capabilities. Specifically, in Chapter IX, "Transform America's National Security Institutions to Meet the Challenges and Opportunities of the 21st Century," the *NSS* directs the DoD "to continue current transformation efforts detailed in the 2006 *QDR*."[17] The *QDR*, which provides strategic guidance for defense transformation, lists achieving network-centric operations as a key joint force operational capability.

The *NDS* builds upon the *NSS*, providing overarching guidance defining strategic military objectives. The *NDS* describes what capabilities are required and how they will achieve the strategic military objectives. Conducting network-centric operations appears, in the *NDS,* as one of eight

[15] U.S. Department of Defense, *Defense Secretary of Defense Memorandum, Subject: Capability Portfolio Management Test Case Roles, Responsibilities, Authorities, and Approaches* (Washington, D.C.: Office of the Secretary of Defense, September 16, 2001), 1.
[16] U.S. Department of Defense, *Quadrennial Defense Review Report* (Washington, D.C.: Government Printing Office, 2006), 68.
[17] U.S. Department of Defense, *The National Security Strategy of the United States of America* (Washington, D.C.: Government Printing Office, 2006), 43.

joint forces key operational capabilities that require focus for DoD transformation.[18] The *NDS* states, "Continuing advances in information and communications technologies hold promise for networking highly distributed joint and combined forces. Network-centric operational capability is achieved by linking compatible information systems with usable data."[19]

The *QDR* also identifies network-centric operations as an initial area for testing the emerging joint acquisition portfolio management approach. The *QDR* provides two fundamental imperatives. The first is "to continue reorienting capabilities and forces to be more agile in war and to prepare for wider asymmetrical challenges."[20] The second is "to implement enterprise-wide changes to force structure, processes, and procedures supporting the Department's strategic strategy."[21]

Under the heading of reorienting capabilities and forces, the *QDR* outlines the vision, progress made to date, and decisions made to realize net-centricity. The vision is "viewing information as an enterprise asset to be protected and information sharing to increase the speed of business processes and decision making."[22] Progress to date includes heavy investment in satellite communications capabilities and the GIG. Decisions made to progress toward the net-centric vision include "strengthening its data strategy...increasing investment in the GIG...developing an information strategy to guide interagency and coalition operations...shift from service efforts to a more department wide enterprise net-centric approach...and further developments in the DoD satellite program."[23] The *QDR* has identified net-centricity as one of the ten joint capability portfolios for managing investment in acquisition programs to facilitate progress toward these initiatives.[24]

[18] U.S. Department of Defense, *The National Defense Strategy of the United States of America*, 12-16.
[19] Ibid., 14.
[20] U.S. Department of Defense, *Quadrennial Defense Review Report*, 1.
[21] Ibid., 1.
[22] Ibid., 58.
[23] Ibid., 59.
[24] Ibid., 41.

The current *NMS* was published in 2004, two years prior to the *NSS* and one year prior to the *NDS*. Despite this disparity in chronological sequencing, the *NMS* captures the concept of developing a network-centric capable joint force. The *NMS* describes network-centric capability as "a networked force capable of decision superiority can collect, analyze, and rapidly disseminate intelligence and other relevant information from the national to tactical levels, then use that information to decide and act faster than opponents."[25] In its description of a joint vision for future warfighting, the *NMS* describes the GIG as "potentially, the single most important enabler of information sharing and decision superiority."[26]

A review of the *NSS*, *NDS*, *QDR*, and *NMS* demonstrates that senior DoD leadership is directing the development of network-centric capabilities. Improved network-centric capabilities support transformation goals by providing linked sensors, weapons, and decision makers operating in global communications architecture. Network-centric capabilities have already demonstrated their effectiveness in improving operations in Afghanistan and Iraq. However, as articulated in national strategic planning documents, improvements have the potential to further enhance the effectiveness of military operations and are a fundamental part of defense transformation. Strengthening data sharing by implementing the *DoD Net-Centric Data Sharing Strategy* is an essential element in developing network-centric capable joint forces.

"Many-to-Many" and "Post and Smart-Pull" Information Environment

"Many-to-many" information exchange is the idea that data is available to all authorized users of the GIG, both those for whom the data was designed as well as unanticipated users.[27] "Post and smart-pull" is the idea that users will post relevant data to shared spaces prior to processing for early use by others, and provides the ability for users to decide what data they desire to pull from the

[25] U.S. Department of Defense. *The National Military Strategy of the United States of America* (Washington, D.C.: Government Printing Office, 2004), 14.
[26] Ibid., 22.
[27] U.S. Department of Defense, *Department of Defense Net-Centric Data Strategy,* 2.

shared space.[28] This is a change of approach from current data management practices in two ways. First, the data from system-to-system interfaces that currently only share information to a finite group of users will post data to a shared data space for other users to access. Second, data posted for a wider audience is now generally processed and exploited before dissemination. The "many-to-many" concept expands data sharing by making more data available to a larger group of users quicker than in the past. Data from the system-to-system exchanges for specified tasks such as a sensor to shooter interface is placed into a shared space accessible to a wider range of users. Information overload, the pushing of more data than is useful to a user making relevant data difficult to discern, is mitigated as users pull data, from shared spaces throughout the GIG, based on the user's information requirements.

The overarching goal in developing net-centric capabilities is to provide decision makers systems that provide accurate awareness of the friendly and enemy battlefield situation through relevant, expeditious information. This enables decision makers to positively influence operations through the ability to make decisions inside the adversary's decision making cycle. Improved data sharing among DoD components is essential to support this overall goal by providing visibility, access, and understanding to greater amounts of data in a "many-to-many" and "post and smart-pull" information environment. The "many-to-many" and "post and smart-pull" data sharing concepts promotes early data sharing and allows users to decide what information they require.[29]

The desire to develop network-centric capabilities has been identified in the national strategy, and resources have been placed against that desire. From 1990 to 2005, the DoD budget for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) has

[28] Alberts, David A. and Hayes, Richard E., *Power to the Edge: Command and Control in the Information Age* (Washington, D.C: Library of Congress, 2003), 78-83.

[29] U.S. Department of Defense. *Department of Defense Net-Centric Data Strategy*, 1-2. Provides description of "many-to-many." Alberts, David A. and Hayes, Richard E., *Power to the Edge: Command and Control in the Information Age*,, 78-83. Provides description of "post and smart-pull."

increased from 10% to 14%, of the total defense budget.[30] From 2001 to 2005, the budget for C4ISR has risen from $35 to $54 billion.[31] Investment in the GIG is expected to cost approximately $34 billion total through 2011.[32]

The Global Information Grid (GIG)

The GIG is the evolving global DoD communications architecture providing users and systems connectivity. The GIG is defined in *Joint Publication 6-0, Joint Communications System* as follows:

> The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for acquiring, processing, storing, transporting, controlling, and presenting information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems ands services, software (including applications), data, security services, other associated services and National Security Systems.[33]

DoD digitization has created a network of networks, within the GIG, of such size and complexity that management and governance process redefinition is necessary to achieve DoD network-centric capable force goals. On April 3, 2003, Lieutenant General Harry D. Raduege, Jr., the Director of DISA, stated to a Congressional Subcommittee that from September 11, 2001 to the date of his testimony that SECRET Internet Protocol Router Network (SIPRNET) capacity increased by 292% and Non-Secure Internet Protocol Router Network (NIPRNET) capacity increased by 509%.[34] The following statistics give an indication of the GIG's size and complexity:

> DoD data systems are comprised of approximately 3.5 million computers running thousands of applications over some 10,000 Local Area Networks (LANs) on 1,500 bases in 65 countries worldwide, connected by 120,000 telecom circuits supporting 35

[30] Gompert, Barry, and Andreassen, *Extending the User's Reach: Responsive Networking for Integrated Military Operations* (Washington, D.C.: National Defense University, 2006),13.
[31] Ibid., 13.
[32] United States Government Accounting Office, *GAO Report-06-211, Defense Acquisitions: DOD Management Approach and Processes Not Well Suited to Support Development of the Global Information Grid* (Washington, D.C.: Government Printing Office, 2006), 2.
[33] U.S. Department of Defense, *Joint Publication 6-0, Joint Communications System* (Washington, D.C.: Government Printing Office, 2006), GL-9.
[34] U.S. Congress, House, Subcommittee on Terrorism, Unconventional Threats and Capabilities House Armed Services Committee. 2003. *Fiscal 2004 Defense Authorization: Information Technology Programs.* Statement by Lieutenant General Harry D. Raduege, Jr., Director, Defense Information Systems Agency. 108th Cong. Accession Number 32Y3808459204.

> major network systems over three router-based architectures transmitting unclassified, secret, and top secret level information.[35]

As a quintessential component for developing network-centric capable joint forces, the GIG and the many DoD component IT systems must be integrated. The proliferation of IT systems throughout the DoD has resulted in the size and complexity of the GIG to a point that procurement governance requires consolidation for cross DoD component GIG initiatives.

Adopting a centralized authority for GIG development efforts is supported by the 2004 findings of the Government Accountability Office (GAO). This 2004 GAO report states that the current decentralized approach to IT procurement does not support developing network-centric capabilities, nor does it provide the DoD CIO adequate influence over DoD component investments, affecting the GIG.[36] In discussing the DoD's decision making processes, the report states, "DoD's major decision-making processes are not structured to support crosscutting, department wide efforts such as the GIG."[37] In the report, the GAO provides the following statement regarding management and governance of the GIG:

> DOD's decentralized management approach for the GIG is not optimized for the development of this type of joint effort, which depends on a high degree of coordination and cooperation. Clear leadership and the authority to enforce investment decisions across organizational lines are needed to achieve the level of coordination and cooperation required, but no on entity is clearly in charge of the GIG or equipped with the requisite authority, and no one entity is accountable for results.....Consequently, the services and defense agencies have relative freedom to align or not align investments with GIG objectives.[38]

[35] Gompert, Barry, and Andreassen, *Extending the User's Reach: Responsive Networking for Integrated Military Operations*, 25.
[36] United States Government Accounting Office, *GAO Report-06-211, Defense Acquisitions: DOD Management Approach and Processes Not Well Suited to Support Development of the Global Information Grid* (Washington, D.C.: Government Printing Office, 2006), 2-5.
[37] Ibid.,14.
[38] Ibid., 3.

Thus, the current *DoD Net-Centric Data Sharing Strategy* represents a cross-cutting department-wide effort in which the DoD CIO does not have adequate influence to optimize data sharing across the GIG.

CHAPTER 3: DEPARTMENT OF DEFENSE NET-CENTRIC DATA STRATEGY

As stated in the Introduction, the purpose of the *DoD Net-Centric Data Strategy* is to strengthen data sharing throughout the DoD by transitioning to a "many-to- many" information environment providing users access to more data than the current information environment which is focused on defined point-to-point interfaces.[39] To institutionalize the objective and goal, as well as provide guidance for implementation of the *DoD Net-Centric Data Strategy*, the ASD/NII DoD CIO published the 2003 *DoD Department of Defense Net-Centric Data Strategy,* the 2004 *DoD Directive 8320.2, Data Sharing in a Net-Centric Department of Defense,* and the 2006 *DoD 8320.02-G, Guidance for Implementing Net-Centric Data Strategy*.

The stated objective of the *DoD Net-Centric Data Strategy* is to improve information sharing by making data more visible, available, and usable, when and where needed, to accelerate decision

[39] U.S. Department of Defense, *Department of Defense Net-Centric Data Strategy*, ii.

cycles.[40] The goal of this strategy is to empower users through faster access to data by posting data to shared space prior to processing.[41] Posting data prior to processing supports the "post and smart-pull" concept, which is the idea that users will post relevant data to shared space prior to processing for early use by others, and users will decide what data they desire to pull from the shared space.[42] Accomplishing the objective and goal of the *DoD Net-Centric Data Strategy* supports national and defense strategic guidance to develop network-centric capable joint forces, and specifically the *QDR* requirement to strengthen the DoD data strategy.

The *DoD Net-Centric Data Strategy* further provides a middle management approach to data management through COIs that are responsible for identification of information sharing capabilities and creation of common discovery and content metadata.[43] COI efforts are supported by GIG Enterprise Services, which is managed by DISA through NCES and provides the metadata formats, metadata repositories, enterprise portals and federated search engines that make data visible, available, and usable to users throughout the GIG. [44] COIs are responsible for the development of data sharing attributes of a program. COIs are also responsible for the development of discovery and content metadata which are data schemes used to identify data stored in shared spaces throughout the GIG. Discovery and content metadata provide the link between the data stored by a data producer and the user searching for data. COIs are then linked to JCIDS and the DAS through interaction between the COI and Joint Portfolio Management Mission Areas to integrate information capabilities into acquisition programs.

The August 2006 *Implementing the Net-Centric Data Strategy Progress and Compliance Report*, published by the DoD CIO, provides an assessment of DoD progress toward achieving data strategy

[40] Ibid., ii.
[41] Ibid., ii.
[42] Alberts, David A. and Hayes, Richard E., *Power to the Edge: Command and Control in the Information Age*, 78-83.
[43] U.S. Department of Defense, *Department of Defense Net-Centric Data Strategy*, 4-6.
[44] Ibid., 6-9.

goals. The assessment, which queried DoD components and agencies, documented four key findings describing areas of progress and areas requiring increased attention to meet the *DoD Net-Centric Data Strategy* goals.[45]

Communities of Interest

COIs are defined in the *DoD Net-Centric Data Strategy* as "collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have shared vocabulary for the information they exchange."[46] The COI will manage the day to day process of integrating data sharing into program development. COIs are committed to actively sharing information recognizing the anticipated, as well as unanticipated users in their development of data sharing concepts.[47] *DoD 8320.02-G* provides the following list of COI primary responsibilities:

> Identify data assets and information sharing capabilities, both operational and developmental that conform to the data strategy goals in the DoD Chief Information Officer Memorandum, *DoD Net-Centric Data Strategy,* May 9, 2003.
>
> Identify approaches to enable those data assets and information sharing capabilities to satisfy data strategy goals and to measure the value to consumers of shared data.
>
> Develop and maintain semantic and structural agreements to ensure data assets can be understood and used effectively by COI members and unanticipated users.
>
> Register appropriate metadata artifacts for use by the COI members and others.
>
> Extend the DoD Discovery Metadata Specification (DDMS) as required to ensure that COI-specific discovery metadata is understandable for enterprise searches.
>
> Partner with governing authority, as appropriate, to ensure that COI recommendations are adapted and implemented through programs, processes, systems and organizations.[48]

[45] U.S. Department of Defense, *Implementing the Net-Centric Data Strategy Progress and Compliance Report* (Washington, D. C.: Government Printing Office, 2006), 7.
[46] U.S. Department of Defense, *Department of Defense Net-Centric Data Strategy,* 4.
[47] U.S. Department of Defense, *Department of Defense 8320.02-G, Guidance for Implementing Net-Centric Data Sharing*, 11.
[48] Ibid., 12.

Until establishment of the *DoD Net-Centric Data Strategy*, data was governed from the top through technical standards and controls of the DoD and administered by DISA. Information sharing capabilities were then built from the bottom up by capability developers meeting established technical standards with requirements focused on system- to-system interfaces. This method of administration is becoming unmanageable due to the size and complexity of the GIG and has led to the development of stove-pipes with direct system-to-system interfaces which do not allow for data to be made readily available, particularly to unanticipated users. COIs, as a middle management approach, will ensure compliance with technical standards while leading capability developers to produce systems based on common discovery and content metadata.

COI membership will include a Governing Authority to provide oversight of COI processes and COI members listed in *DoD Directive 8320-G* include "DoD component representatives, program managers, systems owners, developers, data consumers, DoD component leadership, portfolio managers, and others, all of whom can contribute in different ways to COI activities."[49] Participation may include members of the Joint Staff, JFCOM, the combatant commands, military services, defense agencies, program managers, and capability developers. COIs may form based upon a common data sharing mission areas, such as Joint Command and Control (JC2) or Intelligence, Surveillance, and Reconnaissance (ISR). COI membership will include persons with technical expertise in data sharing solutions and representative program managers, and may also include the actual data producer for the solution in development.[50] COI members will form working groups and technical forums to develop data sharing requirements and solutions.

COI leadership is provided by two key individuals or organizations, the COI Governing Authority and the COI Lead. *DoD 8320.02-G* lists Portfolio Management Mission Area Leads,

[49] Ibid., 12.
[50] Ibid., 11-13.

combatant commands, or functional support agencies as possible Governing Authorities.[51] COI Governing Authorities are responsible for identifying information sharing problems, reviewing COI plans, adjudicating discrepancies across COIs, promoting COI activities to DoD components, and promoting COI activities through the JCIDS, DAS and Planning, Programming, Budgeting and Execution (PPBE) systems.[52] The COI Lead will come from a DoD component and is tasked to manage the COI serving as the advocate for a data sharing solution across the DoD.[53] The COI Lead ensures appropriate member participation in the COI working groups, leads development of plans and milestones, promotes data sharing policies and practices, and identifies measures of success.[54]

COI stakeholders are those persons or organizations with a vested interest in a data sharing solution. Stakeholders may include representatives from the Joint Staff, JFCOM, combatant or functional commands, military departments and agencies directly or indirectly affected by the COI as data users. *DoD 8320.02-G* lists the following stakeholder responsibilities:

> Promote policies across DoD Components in terms of practices and standards in the implementation areas, including those for data tagging, data access services, and registration of metadata artifacts.
>
> Promote the reuse of data access services within programs and systems.
>
> Track DoD Component implementation of DoD Directive 8320.2, *Data Sharing in a Net-Centric Department of Defense*, through COI activities.
>
> Ensure operator/end-user views and needs are represented in COI semantic and structural agreements, contribute to COI requirements gathering processes, and provide feedback on COI-defined information sharing capabilities.[55]

The stakeholder's responsibility is to promote the reuse of data access capabilities within programs and systems. The reuse of data access capabilities is critical to the overall *DoD Net-Centric Data*

[51] Ibid., 12.
[52] Ibid., 12-13.
[53] Ibid., 13.
[54] U.S. Department of Defense, *Department of Defense Directive 8320.02-G, Guidance for Implementing Net-Centric Data Sharing*, 13.
[55] Ibid., 13.

Strategy because it is through the reuse of common discovery and content metadata that COIs can proliferate commonality in data tagging beyond their own COI to programs developed by other COIs.

Capability developers provide technical representatives to the COI with expertise in the development of data sharing agreements and technical approaches.[56] *DoD 8320.02-G* lists the following capability developer responsibilities:

> Identify technical requirements for supporting information sharing capabilities (e.g., common tagging tools) and recommend the necessary programming and budgeting changes for supporting them efficiently.
>
> Participate in COI working groups, particularly as they relate to architectures, standards, and technical specifications.
>
> Identify implementation alternatives, including common or reusable services or technical capabilities.
>
> Identify technical impacts of COI agreements, for example the impact of a data access service on system performance to critical users.
>
> Implement and maintain agreed upon capabilities.
>
> Ensure operator/end-user views and needs are represented in COI semantic and structural agreements.[57]

Data producers and subject matter experts represent programs or organizations that control, create, and/or maintain data assets relevant to the COI. Data producers are typically systems owners or program managers that provide resources to implement data sharing practices in the COI.[58] Subject matter experts are operators or organizations with resident expertise that is germane to the COI program. Data producers and subject matter experts are responsible to the end user by ensuring

[56] Ibid., 13.
[57] Ibid., 13-14.
[58] Ibid., 13-14.

user views are represented in COI semantic agreements. They also provide advice on subject matter priorities and assist in the development of data sharing measures of success.[59]

The process of forming a COI includes identifying its purpose, membership, required information sharing capabilities, structure, and processes.[60] The individual or organizations desiring to form a COI will first seek out stakeholders with a common interest in the information sharing capabilities. The newly formed group will develop a mission statement and charter for guiding COI activities. When considering starting a COI, the COI Lead should consult the COI Directory maintained by GIG Enterprise Services to see if a like COI already exists. This information will guide the COI Lead to either join an operational COI or build upon products developed by a previous COI. If a new COI is to be formed, it should be registered in the COI Directory.[61]

When the decision to form a COI is confirmed, the group must first identify required information sharing capabilities and, second, establish feedback mechanisms to measure success. The COI will identify both mission-specific and mission non-specific measures of success. An example of a mission-specific measure of success is the ability to reduce the time required to plan a strike.[62] An example of a non-mission specific measure of success would be the time saved in fielding a new capability by reusing existing data assets rather than creating new data.[63] Feedback mechanisms should measure success to ensure timely progress in completing tasks and to track changing user needs. The COI should periodically reassess its worthiness over time and only exist as long as the mission is required.[64]

The next step for a COI is to establish a structure and processes to effectively manage its activities. COI members will be assigned responsibilities and tasks required to manage COI

[59] Ibid., 14.
[60] Ibid., 16-22.
[61] Ibid., 16-22. The COI Directory is available at http://gesportal.dod.mil/sites/coidirectory/default.aspx.
[62] Ibid., 17.
[63] Ibid., 17.
[64] Ibid., 16-20.

activities. The processes involved in managing a COI include determining and maintaining mechanisms for information flow, adjudicating issues, prioritizing COI activities, providing quality assurance, interacting with a Portfolio Management Mission Area Lead, and configuration management of COI products.[65]

The COI then establishes necessary working groups to coordinate and execute tasks.[66] Examples of COI working groups include a Joint Implementation Working Group, Pilot Working Group, and Data Management Working Group.[67] The Joint Implementation Working Group is responsible for tasks including developing the COI Capability Roadmap, synchronizing COI activities with the JCIDS process, promoting policies across DoD components, and contributing to COI information gathering processes. The Pilot Working Group is responsible for tasks including demonstrating COI products, executing risk reduction for spiral development, identifying technical requirements for information sharing capabilities, identifying alternative capabilities and the impacts of COI agreements, and ensuring end user views and needs are represented in the COI. The Data Management Working Group is responsible for tasks associated with developing shared vocabulary, ensuring end user views are represented in COI semantic and structural agreements, and maintaining COI data standards.[68]

To ensure COI activities are integrated into JCIDS and DAS for program development and approval, the COI Lead will coordinate with the COI Governing Authority and appropriate Mission Area Lead. The COI Governing authority provides influence across DoD components and the programming and budgeting process to support COI activities. The Mission Area Lead supports movement of required actions through designated Functional Capability Boards (FCB) and the Joint

[65] Ibid., 16-20.
[66] Ibid., 18-19
[67] COI NII Presentation, *Enabling Net-Centric Operations: COI Basics,* available at http://www.dod.mil/nii/cio, 1-14.
[68] Ibid., 1-14.

Requirements Oversight Council (JROC) in the JCIDS process. This interaction will ensure actions are completed in order to reach Milestone Decisions as programs progress through JCIDS and DAS.

Metadata

Discovery and Content Metadata is used to describe the content, format, classification and source of data assets. Commonly referred to as "data tagging" or "data about data," discovery and content metadata is data used to identify and search for data assets stored, in shared spaces, throughout the GIG. Shared space is the location within the GIG where a data asset is located and made available for a user to "pull" from the network. An example of a shared space would be a server at a combatant command that is receiving and storing data in many formats, from database to imagery files. Discovery and content metadata is the technical link between the user searching for a data asset and the data asset stored in a shared space.

Metadata is more complicated than the oversimplified phrase of "data about data." Metadata is defined by the National Information Standards Organization (NISO) as "structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource."[69] An information resource as described in the NISO definition is referred to as a data asset in the *DoD Net-Centric Data Strategy*.

Discovery and content metadata include ontology and taxonomy. The *Net-Centric Data Strategy* describes ontology as including "data categorization schemes, thesauruses, vocabularies, key word lists, and taxonomies."[70] In general terms, ontology provides the elements of metadata used by search engines to find a data asset associated with a data category or a key word. Taxonomies provide a construct or hierarchical format for metadata elements to assist users and software applications in the retrieval of data assets. In general terms, it provides a tiered format for the words

[69] National Information Standards Organization (NISO), *Understanding Metadata* (Bethesda: NISO Press, 2004), 1. NISO is a non-profit association accredited by the American National Standards Institute to identify, develop, maintain, and publish technical standards to manage information.

[70] U.S. Department of Defense. *Department of Defense Net-Centric Data Strategy,* 15.

and definitions used in the vocabulary that will be used to search for data assets in the shared spaces. *DoD 8320.02-G* describes taxonomy as "a categorization hierarchy indicating generalization and specialization relationships between terms; a submarine is a kind of sea based asset, and an Abrams M1A1 is a kind of tank."[71]

Associating discovery and content metadata can be completed physically by including discovery and content metadata in the data asset or by logically associating the data asset with an Extensible Markup Language (XML) file that describes the data asset.[72] Figure 1 is an XML metadata example associated with an imagery data asset in Kabul. From this example, the hierarchal nature of the metadata is evident.

```
<?xml version="1.0 encoding="UTF-8"?
<metadata xmlns:xsi="http://www.w3.org/2001/XMLScheme-instance"
xsi:noNameSpaceSchemeLocation="Intel_Imagery.xsd">
   <mil.af.rl.jbi.Intel_Imagery/>
   <RequiredMetadata>
       <Type>Imagery</Type>
       <JBIIdentifier>JBI000023</JBIIdentifier>
       <publisher>418th</publisher>
       <keywords>Intel,/keywords>
       <language>EN</language>
   <RequiredMetadata>
   <ImageDescriptor>
        <ImageType>IR</ImageType>
        <Area>Kabul</Area>
        <LocationCoord>
            <lat>33.34</lat>
            <latord>N</latrod>
            <long>69.98</long>
            <longord>E</longord>
         </LocationCoord>
     </ImageDescriptor>
</metadata>
```

[71] Ibid., 30.
[72] Ibid., 25.

Figure 1[73]

Deputy Secretary of Defense Management Initiative Decision (MID) 905 required all Military Departments and Agencies to register metadata in the DoD Metadata Registry by September 2003.[74] *DoD Directive 8320.2* directs that all discovery metadata conform to the DoD Discovery Metadata Specification, and that it comply with national and international standards whenever possible.[75] Metadata stored in the DoD Metadata Registry advertises existing metadata providing the opportunity for COIs to reuse previously registered metadata. If COIs reuse discovery and content metadata as suggested, data sharing will improve with the standardization of definitions, categorizations, and vocabulary used to reference data assets.

The *DoD Net-Centric Data Strategy* uses a library analogy to describe this process of posting and sharing metadata.[76] The DoD Metadata Registry is analogous to the library card catalog, with empty formatted cards for COIs to fill out with metadata and containing cards previously filled out by other COIs. COIs building new metadata review the previously filled out cards that can be used in its metadata to promote data sharing. COIs then complete and post new cards in the directed format to describe the formats, definitions, vocabulary, and thesaurus information about the data. The DoD Metadata Registry provides the repository for metadata recorded on the cards.

The metadata stored on the card is also used to tag data assets available, in shared space, within the GIG. These shared spaces are analogous to the library bookshelves. Metadata with its

[73] Mark Linderman and others, eds., *Joint Battlespace Infosphere (JBI): Information Management in a Net-Centric Environment* (Rome, New York: Air Force Research Library, 2006), 5. The Joint Battlespace Infosphere is an information management concept developed by the Air Force Scientific Advisory Board to address information management challenges in the military environment.

[74] U.S. Department of Defense, *Department of Defense Memorandum Subject: DoD Net-Centric Data Management Strategy: Metadata Registration* (Washington, D.C.: Government Printing Office, 2003), 1. This memorandum is signed by John P. Stenbit, DoD Chief Information Officer.

[75] U.S. Department of Defense, *Department of Defense Directive 8320.2, Data Sharing in a Net-Centric Department of Defense* (Government Printing Office, 2004), 2. The DoD Discovery Metadata Specification is located in the DoD Metadata Registry http://diides.ncr.disa.mil/mregHomePage.portal.

[76] U.S. Department of Defense. *Department of Defense Net-Centric Data Strategy,* 7-8.

associated data assets is stored on the bookshelves.[77] Search portals or software applications are used by the GIG users to locate and access the data assets in the shared space.

COI compliance with DoD Discovery Metadata Standards (DDMS) requirements, creation and registration of metadata in the DoD Metadata Registry, and the proliferation of common metadata structures is essential to developing a GIG populated with visible, accessible, and understandable data. Data assets are made accessible by posting the data assets to shared space with associated metadata.

GIG Enterprise Services (GES)

Users of the GIG will use GIG Enterprise Services (GES) to search and pull data from shared space. GES is managed by DISA to support enterprise-wide information services for the DoD through Net-Centric Enterprise Services (NCES). GES is an essential component to the *DoD Net-Centric Data Strategy* and is developing enhanced services under its emerging NCES program. Currently, NCES provides services through three portal product line capabilities: enterprise collaboration, enterprise portal, and content discovery and delivery.[78] Enterprise collaboration provides collaborative tools, such as text collaboration and web conferencing. Text collaboration includes chat and instant messaging services. Web conferencing provides audio and video conference sessions, as well as white boarding services. The enterprise portal provides authorized user access to designated portals throughout the GIG. Content discovery and delivery services provide search services for users to find data. These services also provide enterprise catalog services to store and retrieve metadata and enterprise content delivery services to support the storage and forward staging of information for fast access. NCES is also responsible for providing the DoD

[77] Ibid., 7-8.

[78] U.S. Department of Defense, Defense Information Systems Agency, *Net-Centric Enterprise Services (NCES)* (Washington D.C.: Government Printing Office, 2006). Available on the DISA Webpage at http://www.disa.mil/nces/about_nces/ Program Overview Brief.pdf.

Metadata Registry using technical specifications from the International Organization for Standards (ISO) 11179, the DoD XML registry, and the Defense Data Dictionary System (DDDS) as references for COI metadata developers.[79]

Net-Centric Data Strategy Progress and Compliance Report

In August 2006, the DoD CIO published *Implementing the Net-Centric Data Strategy Progress and Compliance Report*, providing an assessment of DoD progress toward achieving data strategy goals. The assessment, conducted by ASD/NII DoD CIO, queried DoD components and agencies focusing on four areas: Net-Centric Data Strategy Goals, COIs, institutionalization, and recommendations.[80] The assessment showed that the DoD components and agencies are moving forward with initiatives to achieve Net-Centric Data Strategy goals. However, some areas require increased attention by the DoD to maximize the effectiveness of these initiatives. The areas requiring attention were captured in four findings:

> Finding 1: The value of the Net-Centric Data Strategy remains largely unrealized by the warfighter, business and intelligence operators. The Department does not have a systematic process for measuring implementation progress against the Net-centric Data Strategy goals, collecting empirical evidence documenting the value of the Net-Centric Data Strategy to the operator or assessing unsatisfied data needs."
>
> Finding 2: Communities of interest (COIs) are being established but require greater cross-DoD Component participation to address data sharing problems that cross organizational boundaries. In addition, COIs lack a structured mechanism for informing the Department's portfolio management process relative to information sharing decisions.
>
> Finding 3: The DoD Components are updating their respective policies and guidance to reflect the Net-Centric Data Strategy goals; they are primarily focused on implementing the goal of understandability and require additional technical guidance to mature implementation of the visibility and accessibility goals.
>
> Finding 4: The Joint Capabilities Integration and Development System (JCIDS); Defense Acquisition System (DAS); and Program, Planning, Budgeting, and

[79] U.S. Department of Defense. *Department of Defense Directive 8320.02-G, Guidance for Implementing Net-Centric Data Sharing*, 8.

[80] U.S. Department of Defense, *Implementing the Net-Centric Data Strategy Progress and Compliance Report* (Washington, D. C.: Government Printing Office, 2006), 7.

> Execution (PPBE) are overwhelmingly "program-focused" and do not provide needed models for identifying, acquiring, and resourcing net-centric information sharing capabilities.[81]

The ASD(NII) DoD CIO has made recommendations and initiated actions to address the four findings from the *DoD Implementing the Net-Centric Data Strategy Progress and Compliance Report*. These recommendations and actions include efforts by DoD CIO to develop an enterprise-wide data sharing plan, establishment of mission area governance processes for CIOs, DISA development of federated search specifications with detailed technical guidance to describe how to make various data assets visible, and changes to JCIDS and DAS policies to support *DoD Net-Centric Data Strategy* goals.[82]

To develop systematic processes to measure effectiveness in implementation of the *DoD Net-Centric Data Strategy*, the DoD CIO will develop an enterprise-wide data sharing plan including the establishment of an Information Sharing Operations Center.[83] This plan will take into consideration the information sharing needs of DoD, non-federal, and coalition partners. The plan will also emphasize information sharing in the operational environment and provide to metrics to assess the effectiveness of information sharing. To support this plan and assist warfighters in realizing the benefits of the strategy, the Commander, Strategic Command (STRATCOM) and Director of DISA will establish an Information Sharing Operations Center.[84] The center will "assist operators, and the DoD components that implement data sharing capabilities as data sharing issues are encountered in the execution of their missions. The center will provide technical and operational guidance for resolving data sharing problems."[85] The concept of operations for the Information Sharing

[81] Ibid., 1-5.
[82] Ibid., 1-6.
[83] Ibid., 2.
[84] Ibid., 2.
[85] Ibid., 2.

Operations Center includes the development of capabilities to monitor data sharing capabilities including near-real time metrics on data sharing.[86]

Mission Area Leads have been issued guidance by the DoD CIO to increase cross-DoD component participation in COIs to address data sharing problems that cross DoD component boundaries and provide structured mechanisms for notification of portfolio management processes relative to data sharing. Mission Area Leads have been directed to designate a DoD component lead within 30 days of establishing a COI, direct COIs to address identified cross-DoD component information sharing problems, and establish COI governance processes.[87] Mission Area Leads are also responsible for developing mission area specific plans to assess the effectiveness of data sharing implementation.

To address issues presented in Finding 3, DISA and the Defense Intelligence Agency (DIA) will jointly publish a federated search specification, providing guidance to DoD components for publishing their discovery metadata as well as technical guidance describing how to make data assets accessible.[88] No later than 120 days after receiving the federated search specification and technical guidance on data asset accessibility, DoD components are to provide a strategy for making data more visible, accessible, and understandable consistent with Mission Area data sharing priorities.[89]

To resolve issues discussed in Finding 4, changes are planned to JCIDS, DAS, and PPBE systems to orient guidance to a more "net-centric" acquisition approach. The DoD CIO assessment is that the Chairman Joint Chiefs of Staff Instruction (CJCSI), DoD Directive, and DoD Instruction requirements do not include adequate detail in data sharing requirements to support the *DoD Net-*

[86] Ibid., 2.
[87] Ibid., 3.
[88] Ibid., 4.
[89] Ibid., 4-5.

Centric Data Strategy.[90] The *DoD Implementing the Net-Centric Data Strategy Progress and Compliance report* states:

> These policies require programs to describe their relationship to the enterprise from a systems perspective; however, there are only minimum requirements for programs to describe "how" their information is made accessible to the enterprise. These policy documents, against which programs are directed to comply, contain few verifiable elements of the Net-Centric Data Strategy.[91]

In response to these problems, some policy changes are planned and some have recently been published. Planned changes in JCIDS and DAS will ensure NR-KPPs and ISPs include appropriate compliance measures to reflect *DoD Net-Centric Data Strategy* goals and include provisions to ensure capability developers identify their approach to make data visible, accessible, and understandable in JCIDS documentation prior to achieving a Milestone A approval.[92] Recently published changes include *DoD Instruction 8115.02,* which provides detailed guidance for Mission Area Leads on the oversight of portfolios and sub-portfolios with the requirement to ensure portfolio management enables data sharing by linking net-centric criteria to mission area requirements.[93]

Despite the problems presented in Findings 1 through 4, the *DoD Implementing the Net-Centric Data Strategy Progress and Compliance Report* documents significant progress toward development of data sharing policies and procedures by DISA, mission areas, and DoD components. These DoD Agencies, mission areas, and DoD component programs represent a mixture of cross-DoD component and DoD component-specific initiatives. Mission areas have made significant progress in achieving cross-DoD component data sharing goals; however, DoD component efforts remain

[90] Ibid., 5.
[91] Ibid., 5.
[92] Ibid., 6.
[93] U.S. Department of Defense, *Department of Defense Instruction 8115.02, Information Technology Portfolio Management Implementation* (Washington, D.C.: Government Printing Office, 2006), 7.

predominately component focused lacking policies, processes, and incentives engage with cross-component COIs.[94]

An example of a DoD agency initiative is DISA's development of specifications and services for content discovery as part of the Net-Centric Enterprise Services (NCES). NCES Early Capabilities Baseline standardizes approaches for compliance with DoD Discovery Metadata Specification (DDMS) by making the DDMS accessible on the GIG using Federated Search and Enterprise Catalog capabilities.[95] Guidance to COIs and users for using Federated Search and Catalog capabilities is provided in the 2006 *Net-Centric Enterprise Services (NCES) Users Guide*.[96]

The *DoD Implementing the Net-Centric Data Strategy Progress and Compliance Report* noted significant progress at achieving data sharing goals by the Warfighter Mission Area (WMA), Enterprise Information Environment Mission Area (EIEMA), DoD Intelligence Mission Area (DIMA), and the Missile Defense Agency (MDA).[97] The WMA is working on its initial list of data sharing priorities and identifying COIs to manage those priorities. EIEMA has documented the success of several initiatives, including the U.S Army's demonstration of Fusion Net by XVIII Airborne Corps to pass battlefield information to all echelons at the tactical level and the DoD collection and sharing of Improvised Explosive Device (IED) after-action reports from Afghanistan and Iraq.[98] DIMA is formalizing plans for data sharing, having identified its operationally relevant priorities. Based on the DoD CIO report, the MDA is making the most progress at improving data sharing within the realm of internal data sharing requirements of the agency itself. The MDA is working on a directive that will require the registration of all data assets within the mission area. All

[94] U.S. Department of Defense. *Implementing the Net-Centric Data Strategy Progress and Compliance Report,* 2.
[95] Ibid., 13.
[96] U.S. Department of Defense. *Net-Centric Enterprise Services (NCES) Users Guide* (Washington, D.C.: Government Printing Office, 2006), 20-21. This guide is available at http://www.disa.mil.
[97] U.S. Department of Defense. *Implementing the Net-Centric Data Strategy Progress and Compliance Report,* 8.
[98] Ibid., 8.

data will be registered with appropriate metadata in the MDA portal of the DoD Metadata Registry.[99]

DoD component efforts represent a mixture of cross-DoD component and DoD component specific initiatives to develop policies and procedures for data sharing. The *DoD Implementing the Net-Centric Data Strategy Progress and Compliance Report* states:

> DoD Components are establishing COIs to facilitate information sharing across functional areas with a focus on DoD Component priorities. The Military Departments independently govern their COIs through the Air Force's COI Coordination Panel, the Army's COI Harmonization and Integration Forum, and the Department of the Navy's (DON) and United States Marine Corps' (USMC) Functional Area COIs. These types of forums enable the Military Departments to recognize, establish, and reconcile their COIs in relation to their organizational mission needs and priorities.[100]

DoD components are providing data management guidance nested in the *DoD Net-Centric Data Strategy* to their organizations, but are predominately focused on data sharing within their own organizations. These efforts are primarily focused on making data understandable; however, some efforts to improve data visibility and accessibility are in development. Progress in making data understandable has focused on the development of common formats, vocabulary and ontology within the programs under their areas of responsibility. For example, the *Air Force Information Management Strategy Policy* provides guidance to Air Force organizations articulated the Air Force vision for data management.[101] To provide guidance to the Air Force COI coordination panel and lead efforts to make data understandable, the Secretary of the Air Force established the Air Force Data Transparency Initiative Integrated Product Team (IPT).[102] The Army has published guidance in *Army Regulation 25-1, Army Knowledge Management and Information Technology Management* with implementation guidance contained in *Department of the Army Pamphlet, 25-1-1, The Army*

[99] Ibid., 8.
[100] Ibid., 2.
[101] Ibid., 11.
[102] Ibid., 12.

Guidance for Implementing Net-Centric Data Management.[103] Department of the Navy guidance is contained in *SECNAVINT 5000.36A, DON IT Applications and Data Management*.[104] The Defense Logistics Agency (DLA) has published its guidance in *DLA Directive 5025.30*. The following list provides examples of component data sharing initiatives:

> Air Force. The Space Command effort is implementing the C2 SSA vocabulary, developed by the C2 SSA COI, which will provide direct machine to machine communications within six PORs. The effort was established by the Air Force Transparency IPT.
>
> Army. The Army is creating a template for a COI Vocabulary Guide, developing C4ISR Data Ontology, developing the initial XML schema for the BFT COI, and developing a change management plan that supports implementation of the Joint Command, Control and Consultation Information Exchange data Model (JC3IEDM).
>
> USMC. The Marine Corps is developing a Marine Corps-specific ontology to be used internally and externally, across the DoD Components, to ensure semantic correctness within the MCEITS architecture.
>
> Business Transformation Agency (BTA). The BTA published the Standard Financial Information Structure Vocabulary in the DoD Metadata Registry. This vocabulary supports comprehensive corporate financial management and federal financial reporting that is consistent with the Chief Financial Officer Act and is being implemented at the DoD Component level.
>
> DLA. The DLMSO developed the Corporate Logistics Data Architecture that represents the set of logistics data elements under the stewardship of the DOD Logistics Functional Data Administrator. The data elements are structured, named, and defined in accordance with the ISO 11179 standard. The DLA Integrated Data Environment (IDE) used the DDMS.[105]

In addition to the DoD component specific programs, the *DoD Implementing the Net-Centric Data Strategy Progress and Compliance Report* documented the efforts of several DoD component's that will improve joint information sharing. One example is an Air Force led program with Army, Navy and Marine Corps participation called Joint Automated Metadata Tagging Pathfinder, which is

[103] Ibid., 12.
[104] Ibid., 12.
[105] Ibid., 12.

an automated tool for the creation of metadata tags.[106] The program uses a commercial off-the-shelf automation tool to automatically create discovery metadata by searching previously created information on data assets, which will be stored in the metadata repository.[107]

The results of the *DoD Implementing the Net-Centric Data Strategy Compliance Report* demonstrate that the DoD and its components are actively pursuing initiatives to strengthen data sharing. However, analysis of the report also presents a gap in policy regarding the development of mission area and DoD component COI governance practices. While the report mentions that the mission areas and DoD components are moving forward in developing data sharing policies and practices, the report makes no reference to DoD policy changes to guide this effort other than the development of a enterprise-wide data sharing implementation plan.[108] There is no indication that this plan will provide specific guidance, providing unity of effort to mission area and DoD component policies regarding COI governance. Throughout the report, seven mission areas or defense agencies are mentioned as managing or creating COIs; nine Joint COIs are mentioned and a total of 40 DoD component COIs are referenced.[109] These numbers cannot be simply tallied to determine the total number of COIs that currently exist, because the DoD component numbers are intermixed in the mission area and Joint COI numbers. However, the numbers do suggest a decentralized effort that could lead to differences in policy and practices that could limit efficiencies in implementing the *DoD Net-Centric Data Strategy*.

[106] Ibid., 13.
[107] Ibid., 13.
[108] Ibid., 2.
[109] Ibid., 1-16.

CHAPTER 4: THE DEFENSE ACQUISITION PROCESS

The Defense Acquisition System

The Defense Acquisition System (DAS), Joint Capabilities Integration and Development System (JCIDS) and emerging portfolio management guidance are evolving to promote increased network centricity in joint forces and support implementation of the *DoD Net-Centric Data Strategy*. Also, fundamental to the promotion and development of net-centric capabilities and supportive of the *DoD Net-Centric Data Strategy* are the integrated architectures views, Net-Ready Key Performance Parameters (NR-KPP), and the Information Support Plan (ISP).

The DAS contains five major phases of a Major Acquisition Program (MAP) from concept development to final fielding and sustainment. Formal assessments, based on JCIDS documentation, known as Milestone (MS) Decisions are integrated into the process. At these key points in the development of a program, funding approval is received for continued program development. It is at these milestone decisions, listed as A, B, and C, in figure 2, that DoD leadership is presented with the program capabilities, including the ability of the program to support capability and interoperability requirements. For mission critical or mission essential information technology acquisition programs, the DoD CIO certifies that the program is in accordance with subtitle III of Title 40, United States Code, prior to the Milestone Decision Authority (MDA) approval at MS A, B, and C.[110] Figure 2 provides a graphical depiction of the overall framework for the DAS.[111]

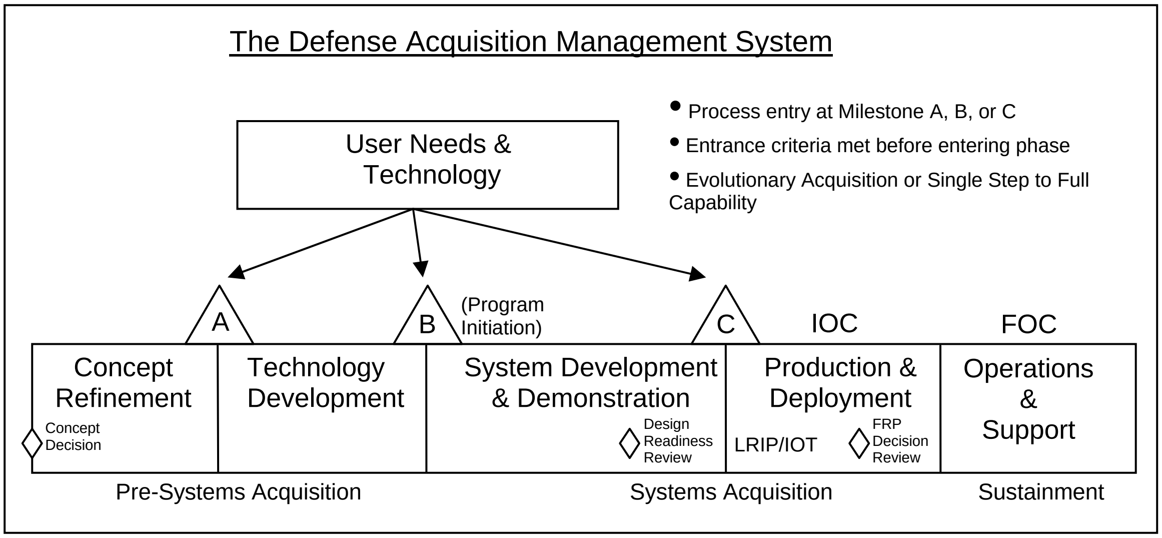

Figure 2

The first phase of the DAS is the Concept Refinement Phase. In this phase, a requirement needed to fill a capability gap is identified. Next, alternatives are proposed and a strategy to develop

[110] U.S. Department of Defense, *Department of Defense Instruction 5000.2, Operation of the Defense Acquisition System* (Washington, D.C.: Government Printing Office, 2003), 18 and 30.
[111] Ibid., 2.

proposed solutions is developed. The first phase officially begins with a Concept Decision approved by the MDA. MDA decisions are documented in an Acquisition Decision Memorandum (ADM) that designates the program lead DoD component or components and provides the initial plan for concept development.[112] The Concept Refinement Phase has three key JCIDS documents associated with it; which are the Initial Capabilities Document (ICD), the Analysis of Alternatives (AoA), and the Technology Development Strategy (TDS). The ICD documents a capability gap that requires resolution to meet a DoD mission requirement. It also evaluates the capability gap across all aspects of Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities (DOTMLPF), which is used to develop an AoA.

The AoA provides assessment of possible material or non-material solutions to meet the mission requirement. The AoA is defined in DoD Instruction 4630.8 which states that an AoA "consists of a broad examination of program alternatives to include technical risk, maturity, and cost. The AoA shall be quantitative and comprehensive, examining the full range of alternatives over the full life cycle to meet the mission requirements, as documented in the associated ICD." [113]

The ICD and AoA are then used to develop the TDS. The TDS provides the overall strategy for system research and development as well as the test plan for spiral or incremental development in an evolutionary acquisition program.[114] Spiral development is the incremental improvement in a program to match new technologies. Incorporation of spiral development into information system programs is designed to ensure that when a program is fielded it does not possess outdated or less effective technology. The Concept Refinement Phase ends when the MDA has approved the AoA and TDS at Milestone A. If an incrementally developed evolutionary acquisition strategy is used, a

[112] Ibid., 6.

[113] U.S Department of Defense, *Department of Defense Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)* (Washington D.C.: Government Printing Office, 2004), 27.

[114] Ibid., 6-7.

revised TDS is required for each increment. An approved MS A decision marks the beginning of the Technology Development Phase.

The Technology Development Phase is the second phase of the DAS. In this phase, the user and the Science and Technology (S&T) communities unite to explore and demonstrate technologies that fulfill ICD documented requirements. Multiple demonstrations of varying technologies may be evaluated prior to identification of the preferred solution. The capstone JCIDS document developed during this phase is the Capability Development Document (CDD). The CDD is a conglomeration of documents that define the incremental capability articulating the requirement into a program that can be produced within a reasonable period of time. *DoD Instruction 5000.2* lists this time as "normally less than five years."[115] Critical components of the CDD to achieve DoD information sharing goals are integrated architecture views, NR-KPPs and the ISP.

The CDD includes integrated architectures in three views: operational, systems, and technical. *DoD Instruction 4630.8* defines these views as follows:

> These views are the Operational View (OV) describing the tasks and activities, operational elements and information exchanges required to accomplish DoD missions; the Systems View (SV) describing (including graphics) systems and interconnections providing for, or supporting DoD functions; and the Technical View (TV) describing the minimum set of rules governing the arrangement, interaction, and interdependence of system parts or elements.[116]

These views are critical in the process of developing and analyzing information sharing requirements for information systems. *DoD Instruction 4630.8* provides the following list of architectural products required for information exchange.[117]

Framework Product and Name	General Description

[115] U.S. Department of Defense, *Department of Defense Instruction 5000.2, Operation of the Defense Acquisition System,* 6.

[116] U.S Department of Defense, *Department of Defense Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),* 25.

[117] Ibid., 27.

AV-1 Overview and Summary Scope, purpose, intended users, environment
Information depicted, analytical findings.

OV-2 Operational Node Operational Nodes, operational activities performed
Connectivity Description at each node, connectivity and information
exchange between nodes.

OV-4 Organizational Organizational, role, or other relationships among
Relationships Chart organizations.

OV-5 Operational Activity Operational activities, relationships among Model
Model activities, inputs and outputs. Overlays can show
cost, performing nodes, or other pertinent
information.

OV-6c Operational Event-Trace One of three products used to describe operational
Description activity sequencing and timing - traces actions in a
scenario of sequence of events and specifies timing
of events.

SV-4 Systems Functionality Functions performed by systems and the Description
information flow among system functions.

SV-5 Operational Activity to Mapping of systems back to operational capabilities
System Function or of system functions back to operational activities.
Traceability Matrix

SV-6 Systems Data Exchange Provides details of systems data being exchanged Matrix
between systems.

TV-1 Technical Standards Profile Extraction of standards that apply to a given
architecture.

KPPs are statements that describe the program's critical characteristics or attributes in a measurable format for use in evaluating program compliance with mandated CDD concepts. *CJCSI 3170.01E* defines KPPs as "attributes or characteristics of a system that are considered critical or essential to the development of an effective military capability and those attributes that make a significant contribution to the key characteristics as defined in the Joint Operations Concepts."[118]

[118] U.S. Department of Defense, *Chairman Joint Chiefs of Staff Instruction 3170.01E, Joint Capabilities Integration and Development System* (Washington, D.C.: Government Printing Office, 2005), GL-12.

Program managers must ensure systems meet or exceed requirements defined in KPPs. NR-KPPs are associated with the system's information sharing characteristics and are a new mechanism to assess interoperability and information sharing capabilities. NR-KPPs are defined in *DoD Instruction 4630.8* as follows:

> The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for the given capability. The NR-KPP, documented in CDDs and CPDs, shall be used in analyzing, identifying, and describing IT and NSS interoperability needs in the ISP; and test strategies in the TEMP.[119]

NR-KPPs must be compliant with the Net-Centric Operations and Warfare (NCOW), Reference Model (RM), and applicable GIG Key Interface Profiles (KIP). The NCOW and GIG KIPs describe and define the activities and standards associated with the system operations and maintenance on the GIG. They include generic network user-interface and configuration control requirements.[120] Compliance with NR-KPPs supports the *DoD Net-Centric Data Strategy* by providing requirements for information sharing across the three integrated views addressed previously. The following is an example of a NR-KPP from the draft Net-Enabled Command Capability (NECC) CDD:

> KPP#4 Net Ready: Net-Ready: They system must support Net-Centric military operations. The system must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The system must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability.[121]

Development Threshold and Development Objective requirements provide detailed information on the Information Exchange Requirements (IER). These IERs are associated with the integrated

[119] U.S Department of Defense, *Department of Defense Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),* 27.
[120] Ibid., 27.
[121] U.S. Department of Defense, *Net-Enabled Command Capability (NECC) Capability Development Document (CDD) (DRAFT) Increment 1* (Washington, D.C.: Government Printing Office, 2006), 25.

architecture views in the NECC program. Additionally, Development Threshold and Development Objectives reference the associated program requirements from the NCOW RM and select GIG KIPs.[122] The NECC CDD identifies 17 KIPs requiring compliance in three categories: communications, computing infrastructure, and enterprise services. KIP 17 relates specifically to the requirement to support applications for data sharing.[123] NR-KPPs and their associated GIG KIPs, are used to develop the information sharing and interoperability requirements in the program's ISP.

The purpose of the ISP is to document the information sharing and interoperability requirements over the life-cycle of the program through the JCIDS process. The ISP is a critical management tool in the JCIDS process because it documents the information sharing and interoperability requirements of an IT system. *DoD Instruction 4630.8* provides guidance on the purpose, development, managerial review, and approval of the ISP. The ISP is a living document that supports evolutionary acquisition by documenting information sharing and interoperability requirements that emerge as new technologies are developed through the life-cycle of the program. The ISP is mandatory for all Acquisition Category (ACAT) and non-ACAT IT programs and is a required with the CDD for a MS B decision. The ISP supports the *DoD Net-Centric Data Strategy* by requiring an assessment of how the system or program will provide information that is accessible and discoverable.

The ISP is developed using the Information needs Discovery and Analysis Process. [124] Figure 3 outlines the steps to this process.[125] Step 7 of the process discusses how the information will be accessed or discovered and relates directly to the *DoD Net-Centric Data Strategy* goals of making data accessible and discoverable.

[122] Ibid., 25.
[123] Ibid,, A-10.
[124] U.S Department of Defense, *Department of Defense Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),* 79-80.
[125] Ibid., 80.

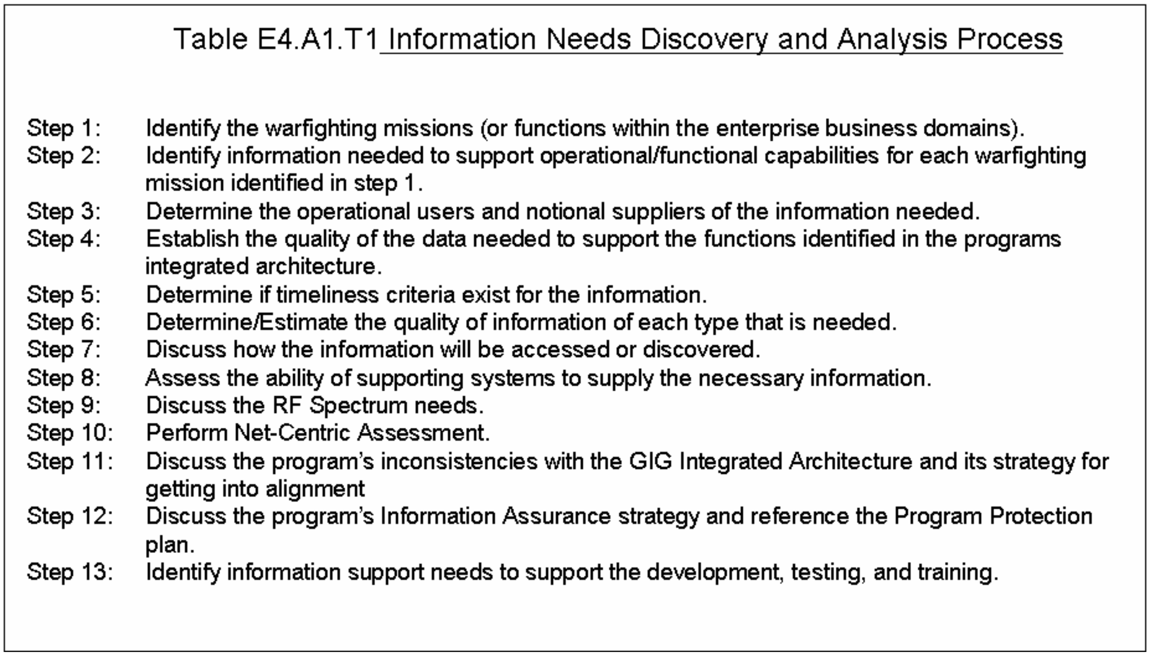

Table E4.A1.T1 Information Needs Discovery and Analysis Process

Step 1: Identify the warfighting missions (or functions within the enterprise business domains).

Step 2: Identify information needed to support operational/functional capabilities for each warfighting mission identified in step 1.

Step 3: Determine the operational users and notional suppliers of the information needed.

Step 4: Establish the quality of the data needed to support the functions identified in the programs integrated architecture.

Step 5: Determine if timeliness criteria exist for the information.

Step 6: Determine/Estimate the quality of information of each type that is needed.

Step 7: Discuss how the information will be accessed or discovered.

Step 8: Assess the ability of supporting systems to supply the necessary information.

Step 9: Discuss the RF Spectrum needs.

Step 10: Perform Net-Centric Assessment.

Step 11: Discuss the program's inconsistencies with the GIG Integrated Architecture and its strategy for getting into alignment

Step 12: Discuss the program's Information Assurance strategy and reference the Program Protection plan.

Step 13: Identify information support needs to support the development, testing, and training.

Figure 3

The ISP review process provides oversight to ensure systems are in compliance with information sharing and interoperability standards. *DoD Instruction 4630.8* states that the "MDA or cognizant fielding authority shall review, assess, and approve ISPs for ACAT II, III, and non-ACAT programs."[126] ACAT I and IA programs receive review by the MDA and are part of the MS B approval for those programs. The ASD(NII) DoD CIO and DISA are participants in the ISP review process and their approval is required for the program to move forward to a milestone decision.[127] DISA, as the DoD Executive Agent for interoperability standards, is part of the review process for all ACAT and non-ACAT programs.[128] The Technology Development Phase ends with the MDA approval of the CDD with its associated integrated architectures, KPPS, ISP, and a Test and Experimentation Plan (TEMP) at MS B. MS B approval is required for each capability increment for a program with an evolutionary acquisition strategy and marks the qualification of a program as

[126] Ibid., 14.

[127] Ibid., 43-65.

[128] Ibid., 43.

an "acquisition program."[129] A MS B approval also means that the program is considered funded in the Planning, Programming, Budgeting, and Execution (PPBE) system with the commitment of monies, personnel, and the assignment of a system to a program manager. The MS B decision marks the beginning of the System Development and Demonstration (SDD) Phase.

The SDD phase begins with the MS B decision and ends with the MS C decision with approval of a program's CPD. The purpose of the SDD phase is to develop the system or incremental capability. In this phase, technological solutions and system prototypes are developed and tested. Systems integration and systems demonstration are the two main sub-phases in the SDD Phase. During systems integration, the S&T and Program Manager communities develop and test technical solutions to meet ICD and CDD capability requirements. It is during systems integration that prototypes are developed and evaluated for their ability to meet all defined requirements articulated in the integrated architectures, KPPs, and ISP in the ICD and CDD.

Upon development of mature prototypes, the system goes through a Design Readiness Review Board (DRR). At this time, the decision is made on whether the system is ready for further prototype development and further testing. The DRR marks the end of the systems integration and the entry into system development in the SDD phase.

During systems demonstration, prototypes are demonstrated and evaluated in the intended operational environment to verify the system meets KPP requirements. It is during this phase that systems go through Initial and Follow on Operational Test and Experimentation (IOT&E and FOT&E).[130] It is during the IOT&E and FOT&E tests that the program manager, supported by a participating unit, tests the system in an operational environment to ensure the system meets KPP requirements. Successful testing in an IOT&E and an approved CPD are required for a MS C

[129] U.S. Department of Defense, *Department of Defense Instruction 5000.2, Operation of the Defense Acquisition System,* 9.

[130] Ibid., 12.

approval. A MS C approval is necessary for the system to enter into the Production and Deployment Phase.

In the Production and Deployment Phase, a system will progress through final operational testing and then enter production. Two major efforts in this phase are Low-Rate Initial Production (LRIP) and Full-Rate Production and Deployment. LRIP is the production of one or a minimal number of systems for final testing. When final testing is complete, the MDA will approval full rate production at a Full-Rate Production Decision Review. Full-Rate Production marks the end of the Production and Deployment Phase and the beginning of the Operations and Support Phase.

The Operations and Support Phase continues through the end of the life cycle of the system and has two main efforts, sustainment and disposal. For an IT system, sustainment includes such activities as data management, configuration management, and information assurance improvements. For an IT system developed with an incremental capability, the system will repeat actions required for a MS B decision through Full-Rate Production. A system is disposed of when it has reached the end of its life cycle or is replaced by a new system. The disposed of system is demilitarized and disposed of in accordance with regulatory and policy guidance.

The Joint Capabilities Integration and Development System

The JCIDS process is a joint top down approach to the analysis and development of systems to meet capability gaps. JCIDS represents a capabilities-based approach to analyzing capabilities as families of systems to promote interdependence and reduce redundancy. JCIDS is linked to the DAS and PPBE system through capability development, review, and approval of JCIDS documentation. This approach is intended to move the acquisition process from a program-centric approach to a capabilities-based approach and gain efficiencies in capabilities at a lower cost, to the DoD.

The JCIDS process begins with the development of Joint Operations Concepts (JOpsC), based on guidance in the *NDS, NMS,* and *QDR*. Desired capabilities are analyzed through a Capability Based

Assessment (CBA) process to determine if a capability gap exists. A capability is defined by *CJCSI 3170.01E* as "the ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks."[131]

The processes for managing capability development by Joint Operations Capabilities (JOpsC) are conducted by a Functional Capabilities Board (FCB).[132] FCBs are managed by the Joint Requirements Oversight Council (JROC).[133] The JROC is the approval authority for ACAT I, IA, or lesser ACAT programs that have been designated as JROC Interest programs due to the systems impact on joint warfighting.[134] A program is assigned an ACAT based upon its cost and degree of joint interdependency. There are four ACATs: I, IA, II, and III. *DoD Instruction 5000.2* provides detailed descriptions of the ACATs, the funding thresholds, and MDA.[135] FCBs work with the program sponsor providing oversight to sponsor activities in the development of the capability and its associated JCIDS documentation. However, the sponsor is ultimately responsible for the analysis associated with the CBA, collaborative planning with other DoD and non-DoD agencies, developing JCIDS documentation, and resolving emerging issues.[136]

The JCIDS and DAS process supports the *DoD Net-Centric Data Strategy* through the development and approval of integrated architectures views, NR-KPPs, and the ISP. These documents define data exchange, interoperability, and information support requirements for a program. These documents are required in key JCIDS documents reviewed during MS decisions and promote integration of program net-centric capabilities.

[131] U.S. Department of Defense, *Chairman Joint Chiefs of Staff Instruction 3170.01E, Joint Capabilities Integration and Development System,* A-7.
[132] Ibid., B-1, B-2.
[133] Ibid., B-1.
[134] Ibid., GL-11.
[135] U.S. Department of Defense, *Department of Defense Instruction 5000.2, Operation of the Defense Acquisition System,* 21.
[136] U.S. Department of Defense, *Chairman Joint Chiefs of Staff Instruction 3170.01E, Joint Capabilities Integration and Development System,* B-3.

CHAPTER 5: RECOMMENDATIONS

To effectively implement the *DoD Net-Centric Data Strategy*, the DoD should establish a Joint COI Working Group responsible for the development of policy and a Joint COI Oversight Council responsible for approval of future Net-Centric Data Strategy policy. The purpose of the Joint COI Working Group would be to develop recommended policy changes based upon the findings in the *Implementing the DoD Net-Centric Data Strategy Progress and Compliance Report* and changes deemed necessary as future data sharing issues and opportunities present themselves. A major effort of the Joint COI Working Group should be to lead the development of discovery and content metadata standards for mission areas and DoD component-like functional areas that are not managed by a mission area.

The purpose of the Joint COI Oversight Council would be to review, direct modifications if required, and approve policy changes recommended by the Joint COI Working Group and to provide oversight of mission area and DoD component COI activities. Establishing a Joint COI Working Group and Joint COI Oversight Council will provide unity of effort in the development of data sharing policy across the DoD. It will also ensure policy from DoD through mission areas and DoD components is mutually supporting and leads to the establishment of a data sharing environment described in the *DoD Net-Centric Data Strategy*.

Both the Joint COI Working Group and the Joint COI Oversight Council should be led by the ASD(NII) DoD CIO supported by the USD(AT&L). Both organizations should include representation from DoD components, defense agencies, geographic combatant commands, functional combatant commands, and mission areas. The Joint COI Working Group should be given the responsibility to develop *DoD Net-Centric Data Strategy* policy and make change recommendations to DoD Directives and Instructions that influence data sharing within the ASD(NII) and USD(AT&L) areas of responsibility. The Joint COI Oversight Council should be empowered to approve changes to DoD Directives and Instructions. The Joint COI Oversight Council Lead and representatives should possess influence necessary to enforce Joint COI Oversight Council decisions within their respective organizations. The authority to enforce policy and adjudicate conflicts will allow the Joint COI Oversight Council to ensure the unity of effort in DoD-wide data sharing programs policies, procedures, and activities.

The Joint COI Working Group should also be responsible for the development of DoD data sharing policy based upon the review of present DoD policy, policy in development and best practices by mission area and DoD components, and future policy, based on advancements in information technology. The working group should then focus on recommending changes to DoD policy that will provide unity of effort between the DoD, mission areas and DoD components. The working group should begin with assessment of policies already under development across the DoD with emphasis on those areas identified in the *Implementing the DoD Data Strategy Progress and Compliance Report*. An effort should be made to develop policies that direct standardization in Mission Area and DoD component policies deemed in the interest of the overall DoD wide goals as stated in the *DoD Net-Centric Data Strategy*.

Three areas of policy that require immediate attention by the Joint COI Working Group include; the development of common mission area COI governance policies with standards for mission area discovery and content metadata, policies that direct DoD component participation in Joint COIs, and the development of discovery and content metadata standards for like functional areas not managed by mission areas, as well as changes to JCIDS, DAS, and PPBE systems to develop more net-centric approaches to identifying, acquiring, and resourcing net-centric information sharing capabilities. Changes to JCIDS, DAS, and PPBE systems should include the requirement for discovery and content metadata in ISPs to link metadata standards to MS A, B, and C approval. With the exception of development of discovery and content metadata standards, these three policy issues were identified as requiring attention in the *DoD Implementing the Net-Centric Data Strategy Progress and Compliance Report.*[137]

The first policy area that requires attention by the Joint COI Working Group is the development of DoD policy for mission area creation of COI governance processes. The Joint COI Working Group should be responsible for developing DoD policy that promotes data sharing across mission area and DoD component boundaries, including the development of discovery and content metadata standards for each mission area. DoD guidance that provides standard practices, required by all mission areas in the governance of their COIs and in specific requirements for discovery and content metadata standards, will ensure cross mission area and DoD component data sharing is a priority as mission areas develop their governance policies. Mission Area Leads have been directed to develop processes to provide governance for their COIs. However, as stated previously, the *Implementing the DoD Data Strategy Progress and Compliance Report* identifies seven different mission areas and defense agencies managing COIs and specifically mentions nine Joint COIs. This situation presents the potential for the development of mission area COI governance policies that do not consider data sharing across mission areas and DoD component COIs outside their respective mission area. Developing DoD guidance that provides unity of effort in mission area development of COI

[137] U.S. Department of Defense. *Implementing the Net-Centric Data Strategy Progress and Compliance Report*, 1-4.

governance processes, with specific requirements for the development of discovery and content metadata standards, will promote data sharing across mission area and DoD component boundaries and ensure policies throughout the DoD support the *DoD Net-Centric Data Strategy* goals.

The second policy area that requires attention is the development of policy which directs DoD component participation in joint COIs. This new policy should include the requirement for Joint COIs to develop discovery and content metadata standards for functional areas that cross DoD boundaries but are not managed by a mission area. The *Implementing the DoD Net-Centric Data Strategy Progress and Compliance Report* states that "DoD Components are establishing COIs to facilitate information sharing across functional areas with a focus on DoD Component priorities....The DoD Components lack the mature policies, processes, and incentives necessary to initiate and engage in joint COIs to address shared data problems."[138] The Joint COI Working Group should be held responsible for the evaluation of DoD component participation in joint COIs and the activities of DoD component COIs in like functional areas, such as logistics or command and control. The Joint COI Working Group should then work with the DoD components to promote participation in Joint COIs and recommend policy changes to promote common data sharing practices. Specifically, the Joint COI Working Group should identify functional areas that cross DoD component boundaries but which are not managed by a mission area in order to develop discovery and content metadata standards for them as well. Conflicts between Joint COI Working Group recommendations and DoD components will be elevated to the Joint COI Oversight Council for adjudication.

The third area involves policy changes to JCIDS, DAS, and PPBE systems to develop more net-centric approaches to identifying, acquiring, and resourcing net-centric information sharing capabilities. These changes should include the requirement for discovery and content metadata in

[138] Ibid., 2.

ISPs in order to link metadata standards to MS A, B, and C approval. This area was identified as Finding 4 in the *DoD Implementing the Net-Centric Data Strategy Progress and Compliance Report*.[139] The report included the following three recommendations related to Finding 4:

> In the next update CJCSI 3170, the Joint Staff (J-8) will include a requirement for identifying potential data challenges early in the JCIDS capabilities analysis process (i.e., Pre-MS A and B) to be included as part of the ICD.
>
> Within 180 days, the DoD CIO, working with the Joint Staff (J-6) and Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), will initiate a review and synchronization of CJCSI 6212, DoDD 4630.5, and DoDI 4630.8, to ensure NR-KPPs and ISPs include appropriate compliance measures that reflect implementation of the Net-Centric Data Strategy as codified in DoDD 8320.2 (includes refinement of required architecture products and policies).
>
> Within 90 days, USD (AT&L) and the DoD CIO will include a requirement in DoDI 5000.2 for programs to describe in the Technology Development Strategy (before MS A) their approach for ensuring that data will be made visible, accessible, and understandable. In addition, both DoDI 5000.2 and DoDI 4630 ill be updated to include specific reference to DoDD 8320.2.[140]

The Joint COI Working Group should monitor development and assess the effectiveness of these changes to Chairman Joint Chiefs of Staff Instruction (CJCSI), DoD Directives, and DoD Instructions as they are published.

In addition to these recommendations, the Joint COI Working Group should recommend changes regarding the inclusion of discovery and content metadata in JCIDS documentation. Currently, *DoD Instruction 4630.8* does not specifically require discovery and content metadata as a requirement in the ISP. DoD components are required to prepare ISPs documenting program interoperability, information, and support requirements for all ACAT and non-ACAT IT programs.[141] ISPs are a mandatory component to ICD, CDD, and CPD JCIDS documents required for Milestone A, B, and C

[139] Ibid., 5.

[140] Ibid., 6.

[141] U.S Department of Defense, *Department of Defense Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),* 29-38.

decisions.[142] *DoD Instruction 4630.8* requires DISA to review all ISPs and the ASD(NII) DoD CIO to review ISPs for ACAT I, ACAT IA, as well as programs designated as special interest.[143]

Changes to JCIDS and DAS policy should require inclusion of a discovery and content metadata plan in the ISP of the ICD and specific discovery and content metadata ontology and taxonomy in the ISP of the CDD and CPD. This will ensure a discovery and content metadata plan is completed for a MS A decision and discovery and content metadata with ontology and taxonomy for MS B and C decisions. Requiring standardization of discovery and content metadata within mission areas and DoD component functional areas will enforce the development of common discovery and content metadata by capability developers. Incorporating discovery and content metadata into ISPs will ensure discovery and content metadata receive adequate oversight in JCIDS and DAS in addition to linking compliance to funding during MS A, B, and C decisions.

In addition to development of policies listed in the first three areas of immediate concern, the Joint COI Working Group should integrate advancements in information technology, best practices observed throughout the DoD, and lessons learned from STRATCOM's Information Sharing Operations Center into policy when beneficial to achieving *DoD Net-Centric Data Strategy* goals. Advances in information technology are emerging on an approximately 18 month cycle.[144] This phenomenon may introduce data sharing challenges that the Joint COI Working Group can change into opportunities by sharing initiatives that may develop in a single mission area or DoD component COI.

Additionally, the Joint COI Working group can serve as a forum for sharing best practices observed across DoD. A best practice example is the Air Force initiated Joint Automated Metadata

[142] Ibid., 24-32. U.S. Department of Defense, *Department of Defense Instruction 5000.2, Operation of the Defense Acquisition System*, 2-16.

[143] U.S Department of Defense, *Department of Defense Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 43.

[144] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 4th ed. (Washington, D.C: Library of Congress, 2002) 247-250.

Tagging Pathfinder.[145] This program, which includes Army, Navy, and Marine Corps participation, uses a COTS automated tool to search data assets and automatically creates discovery metadata.[146] The *DoD Implementing the Net-Centric Data Strategy Progress and Compliance Report* describes numerous DoD component and agency initiatives to improve data sharing, most with joint participation and all with potential joint integration implications.[147] Leveraging best practices across the DoD and codifying these practices into DoD policy will improve data sharing as DoD components integrate the same best practices into their respective data sharing processes.

The Joint COI Working Group should also monitor resolution of data sharing problems presented by DISA from issues received in the planned Information Sharing Operations Center. The ASD(NII) DoD CIO identified the Information Sharing Operations Center as a center to assist operators and DoD Components with resolving data sharing problems.[148] Monitoring resolution of these data sharing problems and sharing the solutions with mission area and DoD components will strengthen their future data sharing programs.

A Joint COI Oversight Council is necessary to provide oversight of the Joint COI Working Group, mission area, and DoD component COI activities, to approve or recommend modification to Joint COI Working Group policy recommendations, and to ensure approved policy changes are integrated into DoD Directives and Instructions. As stated earlier, the Joint COI Oversight Council members must possess the influence to enforce council decisions within their respective organizations. The Joint COI Oversight Council will provide the authority to enact changes to policy necessary to effectively implement the *DoD Net-Centric Data Strategy*. Additionally, the existence of a Joint COI Oversight Council will positively influence the level of priority and

[145] U.S. Department of Defense. *Implementing the Net-Centric Data Strategy Progress and Compliance Report*, 13.
[146] Ibid., 13.
[147] Ibid., 1-17.
[148] Ibid., 2.

participation the mission areas and DoD components place in the Joint COI Working Group and its activities.

CHAPTER 6: CONCLUSION

In 2003, the ASD(NII) DoD COI published the *DoD Net-Centric Data Strategy* providing guidance to the DoD and its components for the development of data sharing policies and practices throughout the DoD. The objective of this strategy is to make data more visible, accessible, and understandable to users throughout the GIG. In response to this strategy and additional guidance in the 2004 *DoD Directive 8320.2, Data Sharing in a Net-Centric Department of Defense* and *DoD 8320.02-G, Guidance for Implementing Net-Centric Data Strategy*, Portfolio Management Mission Areas and DoD components have moved forward in the development of data sharing policies and practices that support their respective data sharing priorities. The DoD data sharing guidance and DoD- wide efforts to develop data sharing policies and practices represent a critical aspect of creating network-centric capable forces articulated as a requirement in the *NSS*, *NDS*, *NMS*, and *QDR*.

In the three years since the publishing of the *DoD Net-Centric Data Strategy*, mission areas and DoD components have made significant progress in developing policies and strategies to promote data sharing. These efforts represent a range of activities that support joint data sharing within Mission Areas and DoD Component COIs. These mission area and DoD component data sharing initiatives represent a decentralized approach in executing DoD data sharing. Given the size and complexity of the GIG, the rate of GIG capability growth, and the fast pace of advances in information technology, this decentralized approach does not provide the unity of effort in Mission Area and DoD components activities to effectively implement the *DoD Net-Centric Data Strategy*. Further, while this decentralized approach lends itself toward making data more visible, accessible, and understandable among stakeholders within Mission Areas and DoD components, it does not support unanticipated users.

To effectively implement the *DoD Net-Centric Data Strategy,* the DoD should establish a Joint COI Working Group responsible for the development of *DoD Net-Centric Data Strategy* policy and a Joint COI Oversight Council responsible for approval of future Net-Centric Data Strategy policy and which would provide oversight of mission area and DoD component COI activities. The purpose of this Joint COI Working Group is to develop policy changes based upon the findings in the *Implementing the DoD Net-Centric Data Strategy Progress and Compliance Report* and deemed necessary as future data sharing issues or opportunities present themselves. A major effort of the Joint COI Working Group should be the development of discovery and content metadata standards for mission areas and DoD component like functional areas that are not managed by a mission area. The purpose of the Joint COI Oversight Council is to review, direct modifications if required, and approve policy changes recommended by the Joint COI Working Group. Establishing a Joint COI Working Group and Joint COI Oversight Council will provide unity of effort in data sharing policy across the DoD and ensure DoD policy down through mission areas and DoD components is mutually supporting, which in turn will lead to the establishment of a data sharing environment described in the *DoD Net-Centric Data Strategy*.

Net-centricity is the concept that a force is best equipped and trained to execute operations with maximum operational benefits through the use of interoperable communications systems linking sensors, weapons, operators, and decision makers. The *NMS* states that, "a networked force capable of decision superiority can collect, analyze, and rapidly disseminate intelligence and other relevant information from the national to tactical levels, then use that information to decide and act faster than opponents."[149] A strengthened data strategy supports developing net-centricity by making data more visible, accessible, and understandable to a larger community of users throughout the GIG. In its description of a joint vision for future warfighting, the *NMS* describes the GIG as "potentially, the single most important enabler of information sharing and decision superiority."[150]

However, the size and complexity of the GIG and the decentralized approach to GIG governance present challenges to developing net-centric capable forces. The GIG is comprised of approximately 3.5 million computers with thousands of applications operating on over 10,000 Local Area Networks spread over 1,500 bases in 65 countries.[151] Investment in the GIG demonstrates that the size and complexity of the GIG will continue to grow. Adopting a centralized authority for GIG development efforts is supported by the findings of the Government Accountability Office (GAO). The GAO reported that the current decentralized approach to IT procurement supporting the GIG did not effectively support developing network-centric capabilities and did not provide the DoD CIO adequate influence over component investments affecting the GIG.[152] In discussing the DoD's decision making processes, the report states, "DoD's major decision-making processes are not structured to support crosscutting, department wide efforts such as the GIG."[153] The *DoD Net-Centric Data Sharing Strategy* represents a cross-cutting department wide effort, in which the DoD CIO does not have adequate influence to optimize data sharing across the GIG.

[149] U.S. Department of Defense. *The National Military Strategy of the United States of America*, 14.
[150] Ibid., 22.
[151] Gompert, Barry, and Andreassen, *Extending the User's Reach: Responsive Networking for Integrated Military Operations*, 25.
[152] United States Government Accounting Office, *GAO Report-06-211, Defense Acquisitions: DOD Management Approach and Processes Not Well Suited to Support Development of the Global Information Grid* 2-5.
[153] Ibid.,14.

In recognition of the need to strengthen the DoD Data Strategy, the ASD(NII) DoD CIO and USD(AT&L) have published guidance that will improve data sharing across the DoD. ASD(NII) DoD CIO guidance is provided in the *DoD Net-Centric Data Strategy.* This guidance articulates the objectives, goals, and a middle management approach to data management to create a "many-to-many" and "post and smart-pull" information environment. This improves upon the current data sharing environment based predominately on system-to-system interfaces. USD(AT&L) guidance incorporating NR-KPPs in JCIDS and DAS directives and instructions ensures data exchange requirements are in JCIDS documents required for milestone decisions in the DAS process. This ties program approval to funding and ensures programs meet data exchange requirements identified in the NR-KPPs.

The foundation for the data strategy is a middle management approach through COIs, use of common discovery and content metadata schemes, and GIG Enterprise Services.[154] COIs will serve as the primary organization responsible for the development of data sharing attributes in a system or program. A significant task accomplished by COIs is the development of discovery and content metadata. Discovery and content metadata, commonly referred to as "data tagging," are data schemes used to identify data assets stored in shared spaces throughout the GIG. Discovery and content metadata include taxonomy and ontology, which form the structure, vocabulary, and thesaurus information that describe a data asset and is associated with the data asset in shared space. Discovery and content metadata is the technical link between the user searching for a data asset and the data asset stored in shared space. GIG Enterprise Services, managed by DISA through NCES, provide the metadata formats, metadata repositories, enterprise portals and federated search engines that make data visible, available, and usable to users throughout the GIG. COIs are linked to JCIDS

[154] Ibid., 4.

and DAS processes through interaction between the COI and Joint Portfolio Management Mission Areas.

The *DoD Implementing the Net-Centric Data Strategy Progress and Compliance Report* provided an assessment with four key findings concerning *DoD Net-Centric Data Strategy* implementation.[155] The assessment conducted by ASD/NII DoD CIO queried DoD components and agencies, focusing on four areas: Net-Centric Data Strategy goals, COIs, institutionalization, and recommendations.[156] The assessment showed that DoD components and agencies are moving forward with initiatives to achieve Net-Centric Data Strategy goals; however, some areas require increased attention by the DoD. These four key findings focused on the need for a systematic process to measure implementation progress against the *DoD Net-Centric Data Strategy* goals, creating greater cross-DoD participation in Joint COIs and providing mechanisms to inform the DoD portfolio management process on data sharing decisions. The findings also noted the need to provide technical guidance to DoD components promoting development of policies and procedures supporting implementation of visibility and accessibility goals. Finally, the report identified the need to provide models for JCIDS, DAS, and PPBE systems that support net-centric acquisition.[157]

The ASD(NII) DoD CIO provides recommendations for resolving issues presented in each of the four key findings. The report identified two specific recommendations related specifically to data sharing and linkages to JCIDS and DAS. The first recommendation states that the DoD CIO working with the Joint Staff J6 and the USD(AT&L) should review and synchronize applicable DoD Directives and Instructions "to ensure NR-KPPs and ISPs include appropriate compliance measures that reflect implementation of the Net-Centric Data Strategy as codified in DoD 8320.2 (includes

[155] U.S. Department of Defense. *Implementing the Net-Centric Data Strategy Progress and Compliance Report*, 1-6.
[156] Ibid., 7.
[157] Ibid., 1-6.

refinement of required architectures products and policies)."[158] The second recommendation states, "USD(AT&L) and the DoD CIO will include a requirement in DODI 5000.2 for programs to describe in the Technology Development Strategy (before MS A) their approach for ensuring that the data will be made visible, accessible, and understandable."[159] Requiring discovery and content metadata schemes in ISPs is a specific action that supports these two recommendations. Establishing a Joint COI Working Group responsible for developing of discovery and content standards supported by enforcement of those standards in JCIDS and DAS supports resolution of problems across all four findings.

To improve the *DoD Net-Centric Data Strategy*, the DoD must integrate common discovery and content metadata standards into JCIDS and DAS processes. This can be accomplished by developing common discovery and content metadata standards. Developing discovery and content metadata with common vocabularies, taxonomies, and ontologies will promote data sharing as acquisition programs use the same discovery and content metadata elements. Discovery and content metadata standards must be included in JCIDS documentation in order to provide adequate oversight on compliance with discovery and content metadata standards. Requiring discovery and content metadata schemes in the ISP accomplishes this task. ISPs are reviewed by DISA and the ASD(NII) DoD CIO and are a required component in ICDs, CDDs, and CPDs, which are JCIDS documents reviewed during acquisition program milestone decisions. Milestone decision approvals are required at key points during the progression of a program through the DAS and determine if a program will be funded and continue in development.

A Joint COI Working Group supported by the authorities of a Joint COI Oversight Council will also resolve identified data sharing problems and improve DoD-wide policies and procedures. Best

[158] Ibid., 6.
[159] Ibid., 6.

practices can then be integrated DoD-wide into programs. DoD components will then avoid past data sharing problems and integrate known solutions into future programs. DoD and component policies and procedures impacting data sharing will become more comprehensive and nested across the DoD. Compliance with established discovery and content metadata standards will be enforced in JCIDS and DAS processes. The combined effects of these actions will build upon the *DoD Net-Centric Data Strategy*, data exchange requirements in *DoD Instructions 4630.0 and 5000.2* and contribute to making data more visible, accessible, and understandable to anticipated and unanticipated users of the GIG.

Developing discovery and content metadata standards, as well as integrating those standards into JCIDS documentation, will allow more effective management of the GIG. Doing so will provide centralized governance over DoD-wide data sharing effort and will reduce data sharing challenges presented by the current size and complexity of the GIG. The ASD(NII) DoD CIO will possess greater visibility of component data sharing initiatives and be able to better monitor progress of in achieving *DoD Net-Centric Data Strategy* goals. A more synchronized *DoD Net-Centric Data Strategy* effort will also achieve cost efficiencies as redundant COI efforts are reduced and fewer data sharing problems, requiring additional cost to resolve, are experienced by more than one COI.

A Joint COI Working Group and Joint COI Oversight Council with the responsibilities and authorities described in this paper will lead to the effective implementation of the *DoD Net-Centric Data Strategy*. The working group and the oversight council will ensure unity of effort and nesting of data sharing policies throughout the DoD. These forums will also establish discovery and content metadata standards that will increase commonality in data sharing attributes in future programs. Integrating these standards into the ISP will ensure the discovery and content metadata receives proper oversight and will tie compliance with standards to program approval and funding.

APPENDIX 1: ACRONYM LIST

ACAT: Acquisition Category

ADM: Acquisition Decision Memorandum

AoA: Analysis of Alternatives

ASD(NII): Assistant Secretary of Defense for Networks Information and Integration

AWACS: Airborne Warning and Control System

BTA: Business Transformation Agency

CBA: Capability Based Assessment

CIO: Chief Information Officer

CJCSI: Chairman Joint Chiefs of Staff Instruction

CDD: Capability Development Document

CPD: Capability Production Document

COI: Community of Interest

C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

DAS: Defense Acquisition System

DDDS: Defense Data Dictionary System

DDMS: DoD Discovery Metadata Specification

DISA: Defense Information Systems Agency

DISR: Defense Information System Agency Registry

DLA: Defense Logistics Agency

DoD: Department of Defense

DoDD: Department of Defense (DoD) Directive

DoDI: Department of Defense (DoD) Instruction

DIMA: Department of Defense (DoD) Intelligence Mission Area

DON: Department of the Navy

DOTMLPF: Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities

DRR: Defense Readiness Review

EIEMA: Enterprise Information Environment Mission Area

FCB: Functional Capability Board

FOT&E: Final Operational Test and Experimentation

GAO: Government Accounting Office

GES: Global Information Grid (GIG) Enterprise Services

GIG: Global Information Grid

GIG KIP: Global Information Grid Key Interface Profile

ICD: Initial Capabilities Document

IDE: Integrated Data Environment

IED: Improvised Explosive Device

IER: Information Exchange Requirements

IOT&E: Initial Operational Test and Experimentation

IPT: Integrated Product Team

ISO: International Organization for Standards

ISP: Information Support Plan

IT: Information Technology

JCIDS: Joint Capabilities Integration and Development System

JFCOM: Joint Forces Command

JOpsC: Joint Operations Capability

JROC: Joint Requirements Oversight Council

JSTARS: Joint Surveillance Target Attack System

KPP: Key Performance Parameter

LRIP: Low-Rate Initial Production

MAP: Major Acquisition Program

MDA: Milestone Decision Authority

MDA: Missile Defense Agency

MS: Milestone

NCES: Net-Centric Enterprise Services

NCOW: Net-Centric Operations and Warfare

NDS: National Defense Strategy

NECC: Net-Enabled Command Capability

NIPERNET: Non-Secure Internet Protocol Router Network

NMS: National Military Strategy

NR-KPP: Net-Ready Key Performance Parameter

NSS: National Security Strategy

OP: Operational View

POR: Program of Record

PPBE: Planning, Programming, and Budgeting Execution

QDR: Quadrennial Defense Review Report

RM: Reference Model

SDD: Systems Development and Demonstration

SIPRNET: SECRET Internet Protocol Router Network

SOCOM: Special Operations Command

STRATCOM: Strategic Command

SV: Systems View

TDS: Technology Development Strategy

TEMP: Test and Experimentation Plan

TV: Technical View

UAV: Unmanned Aerial Vehicle

USD(AT&L): Under Secretary of Defense for Acquisition, Technology, and Logistics

USMC: United States Marine Corps

WMA: Warfighting Mission Area

XML: Extensible Markup Language

GLOSSARY

Accessible: A data asset is accessible when a human, system, or application may retrieve the data within the asset. Data assets may be made accessible by using shared storage space or web services that expose the business or mission process that generates data in readily consumable forms. (DoD Directive 8320.2, Data Sharing in a Net-Centric Department of Defense)

Acquisition Category (ACAT): Categories established to facilitate decentralized decision-making and execution and compliance with statutorily imposed requirements. ACATs determine the level of review, decision authority and applicable procedures. (CJCSI 3170.01E, Joint Capabilities Integration and Development System (JCIDS))

Analysis of Alternatives (AoA): The evaluation of the performance, operational effectiveness, operational suitability, and estimated costs of alternative systems to meet a mission capability. The AoA assesses the advantages and disadvantages of alternatives being considered to satisfy capabilities, including the sensitivity of each alternative to possible changes in key assumptions or variables. The AoA is one of the key inputs to defining the system capabilities in the capability development document. (CJCSI 3170.01E, JCIDS)

Architecture: A framework or structure that portrays relationships among all the elements of the subject force, system, or activity. (Joint Pub 6-0)

Capability Development Document (CDD): A document that captures the information necessary to develop a proposed program(s), normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable and technically mature capability. (CJCSI 3170.01E, JCIDS)

Capability Production Document (CPD): A document that addresses the production elements specific to a single increment of an acquisition program. (CJCSI 3170.01E, JCIDS)

Communities of Interest: An inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have a shared vocabulary for the information they exchange. Also called COI. (DoD Net-Centric Data Strategy)

Data: A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Data and information are equivalent terms for the purposes of this policy. (DoD Directive 8320.2)

Data Asset: Data asset refers to any entity that is composed of data. For example, a database is a data asset that comprises data records. In this document, "data asset" means system or application output files, databases, documents or web pages. Data asset also includes services that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. (DoD Directive 8320.2)

Similarly, a website that returns data in response to specific queries (e.g. weather.com) would be a data asset.

DoD Component: The DoD components consist of the Office of the Secretary of Defense, the Military Departments, the Chairman Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, DoD field activities and all other organizational entities within the DoD. (CJCSI 3170.01E, JCIDS)

Functional Capabilities Board (FCB): A permanently established body that is responsible for the organization, analysis and prioritization of joint warfighting capabilities within an assigned functional area. (CJCSI 3170.01E, JCIDS)

Global Information Grid (GIG): The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security, services, other associated services and National Security Systems. Also called GIG. (Joint Pub 6-0)

Information: 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (Joint Pub 6-0)

Information Environment: The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. (Joint Pub 6-0)

Information Superiority: The operational advantage derives from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Joint Pub 6-0)

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a component, which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services) and related resources. Not withstanding the above, the term "IT" does not include any equipment that is acquired by a federal contractor incidental to a federal contract. The term "IT" includes National Security Systems. (CJCSI 3170.01E, JCIDS)

Initial Capabilities Document (ICD): Documents the need for a material approach, or an approach that is a combination of material and non-material, to satisfy specific capability gap(s). It defines the capability gap(s) in terms of the functional area, the relevant range of military operations, desired effects, time and doctrine, organization, training, material, leadership, and education, personnel, and facilities (DOTMLPF) and policy implications and constraints. The ICD summarized the results of the DOTMLPF and policy analysis and the required capability. The outcome of an ICD could be one or more joint DCRs or capability development documents. (CJCSI 3170.01E, JCIDS)

Integrated Architecture: An architecture consisting of multiple views or perspectives (operational view, systems view, and technical standards view) that facilitates integration and promotes interoperability across capabilities and among related integrated architectures. (CJCSI 3170.01E, JCIDS)

Interoperability: 1. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. 2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases, (Joint Pub 6-0)

Joint Force: A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander. (CJCSI 3170.01E, JCIDS)

Joint Operations Concepts (JOpsC): The JOpsC is the overarching concept that guides the development of future joint force capabilities. It broadly describes how the joint force is expected to operate 10-20 years in the future in all domains across the range of military operations within a multilateral environment in collaboration with interagency and multinational partners. The JOpsC describes the proposed end states derived from strategy as military problems and the key characteristics of the future joint force. (CJCSI 3170.01E, JCIDS)

Key Performance Parameter (KPP): Those attributes or characteristics of a system that are considered critical or essential to the development of an effective military capability and those attributes that make a significant contribution to the key characteristics as defined in the Joint Operations Concepts. KPPS are validated by the Joint Requirements Oversight Council (JROC) for JROC Interest documents, and by the DoD component for Joint Integration or Independent documents. Capability development and capability production document KPPS are included verbatim in the acquisition program baseline. (CJCSI 3170.01E, JCIDS)

Metadata: Information describing the characteristics of data; data or information about data; or descriptive information about an entity's data, data activities, systems, and holdings. For example discovery metadata is a type of metadata that allows data assets to be found using enterprise search capabilities. (DoD Directive 8320.2)

Metadata Registry: Repository of all metadata related to data structures, models, dictionaries, taxonomies, schema, and other engineering artifacts that are used to support interoperability and understanding through semantic and structural information about the data. A federated metadata registry is one in which multiple registries are jointed electronically through a common interface and exchange structure, thereby effecting a common registry. (DoD Directive 8320.2)

Milestone Decision Authority (MDA): The individual designated, in accordance with criteria established by the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Assistant Secretary of Defense of Defense (Networks and Information Integration) (for Automated Information System acquisition programs) or by the Under Secretary of the Air Force (as the DoD Space MDA) to approve entry of an acquisition program into the next phase. (CJCSI 3170.01E, JCIDS)

Net-Centric: Relating to or representing the attributes of net-centricity. Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes and people) in which data is shared timely and seamlessly among users, applications and platforms. Net-centricity enables substantially improved military situation al awareness and significantly shortened decision-making cycles. (CJCSI 3170.01E, JCIDS)

Net-Ready Key Performance Parameter (NR-KPP): The NR-KPP assesses information needs, information timeliness, information assurance and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following elements. (CJCSI 3170.01E, JCIDS)

a. Compliance with the Net-Centric Operations and Warfare Reference model
b. Compliance with applicable Global Information Grid key interface profiles.
c. Verification of compliance with DoD information assurance requirements.
d. Supporting integrated architecture products required to assess information exchange and use for a given capability.

Ontology: Includes data categorization schemes, thesauruses, vocabularies, key-word lists, and taxonomies. Ontologies promote semantic and syntactic understanding of data. (DoD Net-Centric Data Strategy)

SECRET Internet Protocol Router Network: The worldwide SECRET-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. Also called SIPRNET. (Joint Pub 6-0)

Shared Space: Storage on a file server or in electronic media that is addressable by multiple users or COIs. Also web services that are made available to the enterprise that expose the business or mission processes that generate data in readily consumable forms. (DoD Directive 8320.2)

Standardization: The process by which the Department of Defense achieves the closest practicable cooperation among the Services and Defense agencies for the most efficient use of research, development, and production resources, and agrees to adopt on the broadest possible basis the use of: a. common or compatible operational, administrative, and logistical procedures; b. common or compatible technical procedures and criteria; c. common, compatible, or interchangeable supplies, components, weapons, or equipment; d. common or compatible tactical doctrine with corresponding organizational compatibility. (Joint Pub 6-0)

Taxonomy: Provides categorization of related terms. In doing so, they make use of "class/subclass" relationships (i.e. they are hierarchical in conveying the relationships between categories.) Taxonomies are important to ensuring that searches of discovery metadata and content are targeted. (DoD 8320.02-G, Guidance for Implementing net-Centric Data Sharing)

Understandable: Capable of being comprehended in terms of subject, specific content, relationships, sources, methods, quality, spatial and temporal dimensions, and other factors. (DoD Directive 8320.2)

Visible: Able to be seen, detected, or distinguished and to some extent characterized by humans and/or IT systems, applications, or other processes. (DoD Directive 8320.2)

BIBLIOGRAPHY

Alberts, David S., Garstka, John J., and Stein Frederick P. *Network Centric Warfare: Developing and Leveraging Information Superiority,* 4th ed. Washington, D.C.: Library of Congress, 2002.

Alberts, David S. and Hayes, Richard E. *Power to the Edge: Command and Control in the Information Age.* Washington, D.C: Library of Congress, 2003.

CIO/NII Presentation, *Enabling Net-Centric Operations: COI Basics,* Available at http://dod.mil/nii/cio

Gompert, David C., Barry, Charles L., and Andreassen, Alf A. *Extending the User's Reach: Responsive Networking for Integrated Military Operations,* Washington, D.C.: National Defense University, 2006.

Linderman and others., eds., *Joint Battlespace Infosphere: Information Management in a Netcentric Environment,* Rome, New York: Air Force Research Library, 2006.

Luddy, John. *The Challenge and Promise of Network Centric Warfare,* Arlington: Lexington Institute, 2005.

Murray, Williamson and Scales, Robert H. Jr., *The Iraq War: A Military History,* Cambridge: Belknap Press of Harvard University Press, 2003.

National Information Standards Organization. *Understanding Metadata,* Bethesa: NSIO Press, 2004

Press, Barry. "Net Effect: Barry Press, chief engineer at L-3 Communications Systems West, describes how networked data links enhance situation awareness" *C4ISR: The Journal of Net-Centric Warfare,* (Springfield) Vol. 5, No. 4. (May 2005): 42-45.

U.S. Congress, House, Subcommittee on Terrorism, Unconventional Threats and Capabilities House Armed Services Committee. 2003. *Fiscal 2004 Defense Authorization: Information Technology Programs.* Statement by Lieutenant General Harry D. Raduege, Jr., Director, Defense Information Systems Agency.

U.S. Department of Defense. *Chairman Joint Chiefs of Staff Instruction 3170.01E, Joint Capabilities Integration and Development System,* Washington, D.C.: Government

Printing Office, 2005.

U.S. Department of Defense. *Chief Information Office Memorandum, Subject: DoD Net-Centric Data Strategy,* Washington, D.C.: Government Printing Office, 2003.

U.S. Department of Defense. *Department of Defense Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),* Washington, D.C.: Government Printing Office, 2004.

U.S. Department of Defense. *Department of Defense Directive 5000.1, The Defense Acquisition System,* Washington, D.C.: Government Printing Office, 2003.

U.S. Department of Defense. *Department of Defense Directive 8115.01, Information Technology Portfolio Management,* Washington, D.C.: Government Printing Office, 2005.

U.S. Department of Defense. *Department of Defense Directive 8320.2, Data Sharing in a Net-Centric Department of Defense,* Washington, D.C.: Government Printing Office, 2004.

U.S. Department of Defense. *Department of Defense Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),* Washington, D.C.: Government Printing Office, 2004.

U.S. Department of Defense. *Department of Defense Instruction 5000.2, Operation of the Defense Acquisition System,* Washington, D.C.: Government Printing Office, 2003.

U.S. Department of Defense. *Department of Defense Instruction 8115.02, Information Technology Portfolio Management Implementation,* Washington, D.C.: Government Printing Office, 2006.

U.S. Department of Defense. *Department of Defense Net-Centric Data Strategy,* Washington, D.C.: Government Printing Office, 2003.

U.S. Department of Defense. *Deputy Secretary of Defense Memorandum, Subject: Capability Portfolio Management Test Case Roles, Responsibilities, Authorities, and Approaches,* Washington, D.C.: Office of the Secretary of Defense, 2006.

U.S. Department of Defense, Defense Information Systems Agency. *Net-Centric Enterprise Services (NCES),* Washington, D.C.: Government Printing Office, 2006. available at http://www.disa.mil/nces/about_nces/ProgramOverviewBrief.

U.S. Department of Defense. *Guidance for Implementing Net-Centric Data Sharing DoD 8320.02-G,* Washington, D.C.: Government Printing Office, 2006.

U.S. Department of Defense. *Implementing the Net-Centric Data Strategy Progress and Compliance Report,* Washington, D.C.: Government Printing Office, 2006.

U.S. Department of Defense. *Joint Communications System Campaign Plan,* Washington, D.C.: Government Printing Office, 2006.

U.S. Department of Defense. *Joint Publication 5-0, Joint Operation Planning,* Washington, D.C.: Government Printing Office, 2006.

U.S. Department of Defense. *Joint Publication 6-0, Joint Communications System,* Washington, D.C.: Government Printing Office, 2006.

U.S. Department of Defense. *Joint Vision 2020,* Washington, D.C.: Government Printing Office, June 2000

U.S. Department of Defense. *National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow,* Washington D.C.: Government Printing Office, 2004

U.S. Department of Defense. *Net-Enabled Command Capability (NECC) Capability Development Document (CDD) (DRAFT) Increment 1,* Washington, D.C.: Government Printing Office, 2006.

U.S. Department of Defense. *Office of the Secretary of Defense Memorandum, Subject: Policy for Registration of Extensible Markup Language (XML),* Washington, D.C.: Government Printing Office, 2002.

U.S. Department of Defense. *Quadrennial Defense Review Report.* Washington, D.C.: Government Printing Office, 2006.

U.S. Department of Defense. *The National Defense Strategy of the United States of America,* Washington, D.C.: Government Printing Office, 2005.

U.S. Department of Defense. *The National Security Strategy of the United States of America,* Washington, D.C.: Government Printing Office, 2006.

U.S. Government Accounting Office, *Defense Acquisitions DOD Management Approach and Processes Not Well-Suited to Support Development of Global Information Grid,* Washington, D.C.: Government Printing Office, 2006.

U.S. Government Accounting Office, *GAO Report to Congressional Committees; Military Operations; Recent Campaigns Benefited from Improved Communications and Technology, but Barriers to Continued Progress Remain,* Washington, D.C.: Government Printing Office, 2004.

Van Creveld, Martin, L. *Technology and War: From 2000B.C. to the Present.* New York: The Free Press, 1989.